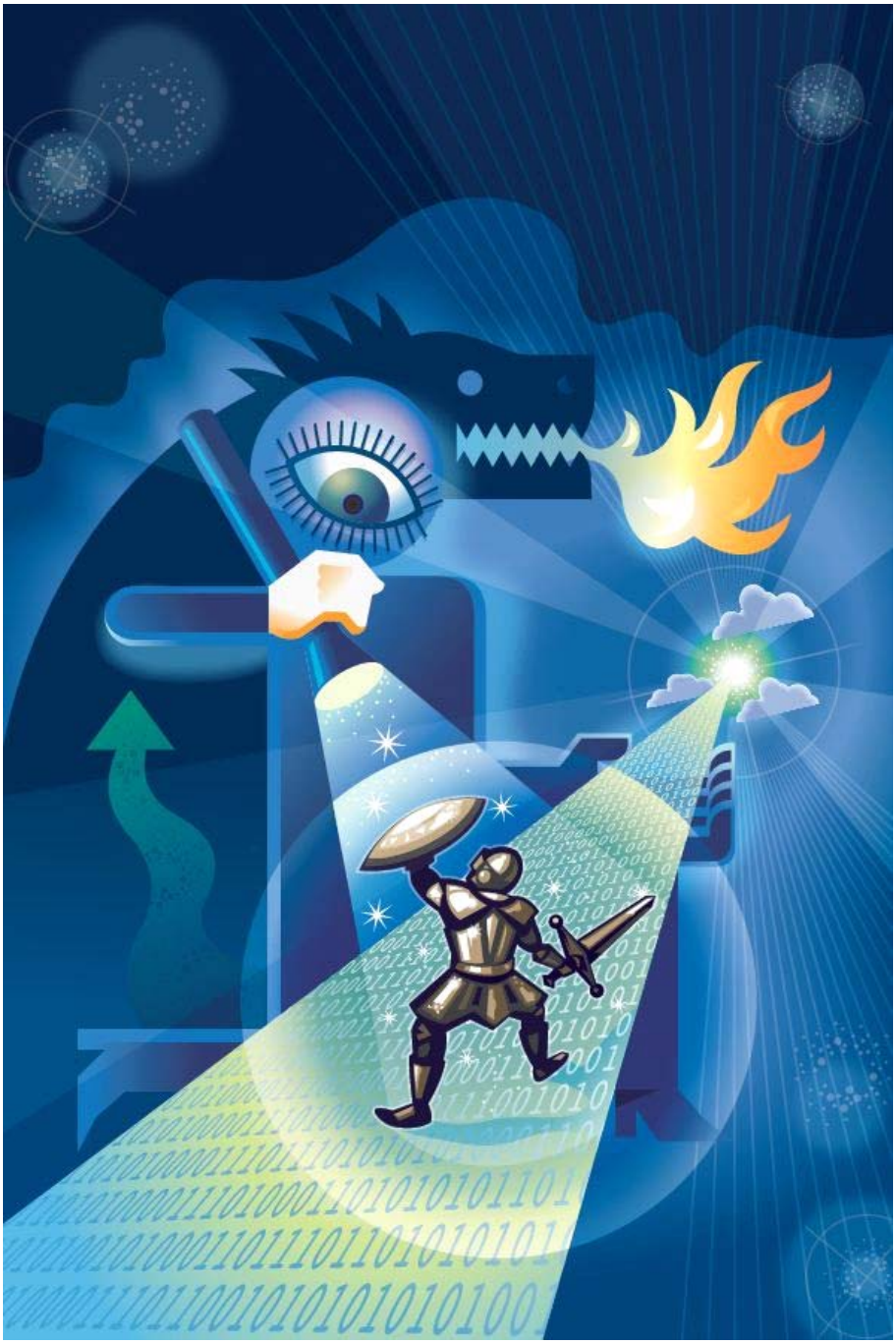
Cisco Compliance Solution for PCI DSS 2.0 Design and Implementation Guide

Third Edition

A Cisco Validated Design



Cisco Validated Design

Solution Authors


Christian Janoff


Bart McGlothin

Christian Janoff, Compliance Solutions Architect, STBU, Cisco Systems

Christian Janoff is a Solution Architect at Cisco Systems with over 15 years of solution architecture and design experience. Christian leads Cisco's participation on the Payment Card Industry Security Standards Council. He was elected to the PCI Council's Board of Advisors in May, 2009. Prior to Cisco, Christian worked as a network engineering manager at Safeway, Inc. Christian holds a bachelor's degree from University of California at Santa Cruz.

Bart McGlothin, Compliance Solutions Architect, STBU, Cisco Systems

Bart McGlothin is a Solution Architect in the Compliance Solutions group at Cisco Systems, Inc. Bart leads the technical aspect of Cisco's SecureX Framework for Compliance and more specifically; Payment Card Industry (PCI) initiatives including Cisco's Validated Designs for PCI compliance. He has over sixteen years of solution architecture and design experience. Bart leads Cisco's involvement with the National Retail Federation's Association for Retail Technology Standards Committee (ARTS) as vice chair of the technical committee and a member of the ARTS board. Prior to Cisco, Bart worked as the Network Architect at Safeway, Inc.

Partner Authors

Rob McIndoe	Aaron Reynolds

Contributors

Mike Adler	Tom Hua
Mark Allen	Raymond Jett
Annette Blum	Manny Kamer
Renata Budko	Rekha Krishna
John Carney	Paul Lysander
Danny Dhillon	Fernando Macias
Michael Dugan	Bob Nusbaum
Zeeshan Farees	Manu Parbhakar
Carol Ferrara-Zarb	Vikram Prabhakar
Syed Ghayer	Jim Rintoul
Sujit Ghosh	Brian Robertson
Manisha Gupta	Angel Shimelish
Jamey Heary	Rick Simon
Gary Halleen	Maria Sisiruca
Stuart Higgins	Sheri Spence
Amanda Holdan	Greg Varga



CONTENTS

CHAPTER 1 **Solution Overview** 1-1

- Executive Summary 1-2
- Target Market/Audience 1-4
- Solution Benefits 1-4
- PCI Solution Results 1-5

CHAPTER 2 **PCI and the Solution Framework** 2-1

- PCI DSS 2.0—New Reporting Guidelines 2-2
- Maintaining PCI Compliance 2-2
- Cardholder Data Environment and Scope 2-3
- PCI Best Practices 2-4
  - Scope Maintenance 2-4
  - Scope Boundary Enforcement 2-6
- Cardholder Data Environment—Scope Layers 2-6
  - Endpoints 2-6
  - Administration 2-7
  - Infrastructure 2-8
- PCI Solution Framework 2-9
  - Endpoints 2-9
  - Administration 2-10
  - Infrastructure 2-10
- Services 2-10

CHAPTER 3 **Solution Architecture** 3-1

- Enterprise Architecture and PCI Design Considerations 3-2
  - Enterprise Network Addressing 3-3
  - Branch Architecture 3-4
  - Data Center 3-7
  - WAN Aggregation 3-9
  - Core Layer 3-11
  - Aggregation Block 3-12
  - Aggregation Layer 3-12
  - Services Layer 3-13

Access Layer 3-14
Host/Server Farm Layer 3-15
Storage Layer 3-17
E-commerce/Internet Edge/Service Provider Edge/Partner Edge 3-18

CHAPTER 4 **Solution Implementation 4-1**

Overview 4-1
Infrastructure 4-2
Branches 4-4
Data Center 4-17
Administration 4-25
Authentication 4-26
Encryption 4-26
Management 4-26
Monitoring 4-27
Endpoints 4-27
Voice 4-27
E-mail 4-28
Physical 4-28
PCI Solution Result Summary 4-29

CHAPTER 5 **Component Assessment 5-1**

Component Section Overview 5-1
PCI Assessment Summary 5-1
Capability Assessment 5-2
Design Considerations 5-4
PCI Assessment Detail 5-4
Endpoints 5-4
Voice 5-4
Physical Security 5-15
E-mail 5-45
Hosts 5-47
Administration 5-65
Authentication 5-65
Management 5-97
Encryption 5-123
Storage 5-131
Monitoring 5-140
Additional In Scope Devices 5-156

Infrastructure 5-156
Routing 5-156
Switching 5-183
Wireless 5-218
Storage 5-235
Security 5-244
Intrusion Detection 5-285

CHAPTER 6 **Summary** 6-1

APPENDIX A **Bill Of Material** A-1
Branch—MSP Branch A-1
Branch—Convenience Branch A-4
Branches—Mini Branch A-5
Branches—Small Branch A-7
Branches—Medium Branch A-10
Branches—Large Branch A-14
Data Center, Internet Edge, DMZ A-19
Data Center—WAN Aggregation A-26
Data Center—Service A-28
Data Center—Secure Storage A-32
Data Center—Extranet Edge A-33
Data Center—Physical Security A-36
Data Center—Wireless Systems A-38
Data Center—Management A-39
Data Center—Access, Aggregation A-40
Data Center—UCS A-43
Data Center—Core A-45

APPENDIX B **Cisco Products and Software Versions** B-1

APPENDIX C **Verizon Business Reference Architecture Report—Cisco PCI Solution** C-1
Table of Contents C-1
Contact Information C-2
1. Executive Summary C-2
Architecture Description C-2
High Level Network Diagram C-3

Quarterly Vulnerability Scans C-4
2. Description of Scope of Work and Approach Taken C-4
PCI DSS Version C-4
Timeframe C-4
Environment on which Assessment Focused (Phase IV & V) C-4
Network Segmentation C-5
Exclusions C-6
Wireless LANs and/or Wireless Applications C-6
List of Individuals Interviewed C-6
List of Documents Reviewed C-7
Build and Maintain a Secure Network C-8
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters C-25
Protect Cardholder Data C-55
Requirement 3: Protect stored cardholder data C-55
Requirement 4: Encrypt transmission of cardholder data across open, public networks C-74
Maintain a Vulnerability Management Program C-77
Requirement 5: Use and regularly update anti-virus software or programs C-77
Requirement 6: Develop and maintain secure systems and applications C-79
Implement Strong Access Control Measures C-93
Requirement 7: Restrict access to cardholder data by business need to know C-93
Requirement 8: Assign a unique ID to each person with computer access C-107
Requirement 9: Restrict physical access to cardholder data C-138
Regularly Monitor and Test Networks C-145
Requirement 10: Track and monitor all access to network resources and cardholder data C-145
Requirement 11: Regularly test security systems and processes. C-188
Maintain an Information Security Policy C-199
Requirement 12: Maintain a policy that addresses information security for all personnel. C-199

APPENDIX D **The Art of Compliance** D-1



CHAPTER 1

Solution Overview

The Payment Card Industry Data Security Standard (PCI DSS) is generally perceived to be a complicated means to secure sensitive information. As of 2010, according to the PCI Security Standards Council, 100 percent of all breached companies were not compliant at the time of the breach, regardless of whether they were compliant at the time of their audit. How did a company that took such pains to achieve compliance not take equal measures to maintain it? Is the standard really so complex that it is not capable of being sustained? Some pundits have argued that PCI is therefore an unrealistic goal and valueless.

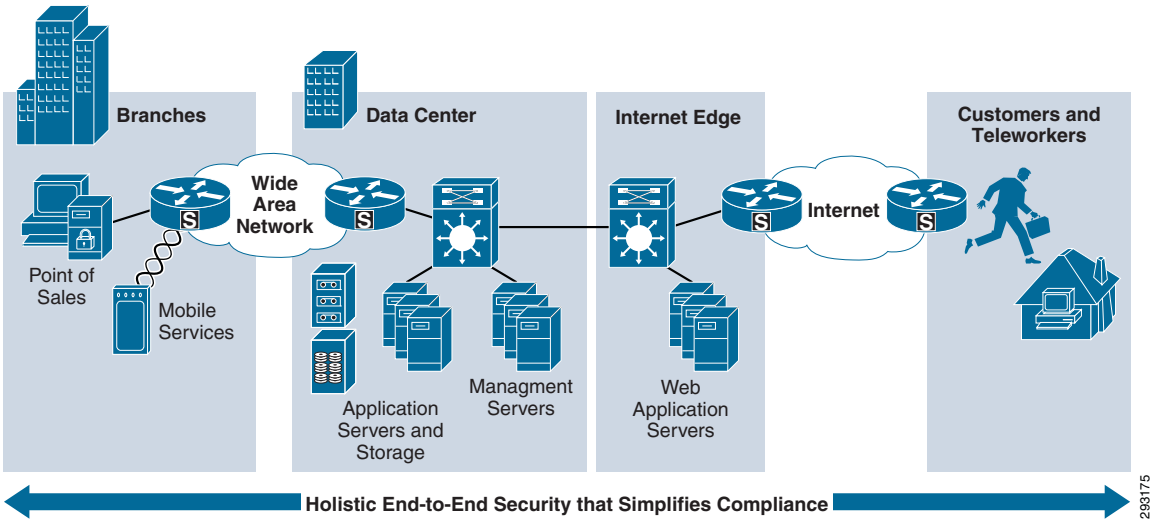
Cisco takes a more balanced stance. PCI is not overly stringent from a security perspective. In fact, Cisco sees the PCI security standard to be the *minimum* security any company should have when taking payments. PCI is a global attempt at setting a minimum bar. Some very large companies and some entire countries have not developed a security awareness that meets the evolved threats of cybersecurity today. From that perspective, PCI is the lowest common denominator that provides the minimum level of protection. Putting in a firewall, changing default passwords, locking the door to the wiring closet, and making sure that you have knowledge of who is configuring a device rather than leaving open a general admin account; these items are not complex.

Although the standard is indeed intricate, the real complexity challenge comes from managing an enterprise network. Enterprise companies do not arise overnight. Most companies that existed in the 1980s did not consider data security to be an ingredient that must be included at all levels. After IP became the de facto network protocol, enterprise companies have been struggling to integrate data with voice systems, video, wireless, digital media, administrative duties, and business processes; as well as holistically integrate protection of payment card information throughout. Each of these technologies was developed independently of each other. With the advent of IP, they have merged, in sometimes inefficient and complex fashion.

Therefore, the real struggle is to develop a simple, sustainable, and operationally efficient enterprise architecture. This foundation needs to have security integrated not only within its technical infrastructure but within its processes and policies as well. This manual is written to provide resources to address these issues and to help simplify compliance.

Figure 1-1 shows the enterprise architecture.

Figure 1-1 Enterprise Architecture



Executive Summary

The Cisco Compliance Solution for PCI DSS 2.0 was developed to help organizations simplify and maintain PCI compliance. The main feature of the solution is *segmentation*. The solution refines a company's compliance needs in the following ways:

- **Defining where sensitive payment information flows**

  This simply means putting sensitive data onto its own network. By segmenting your existing architecture, you can reduce audit costs and simplify maintenance.

- **Protecting the segmented area**

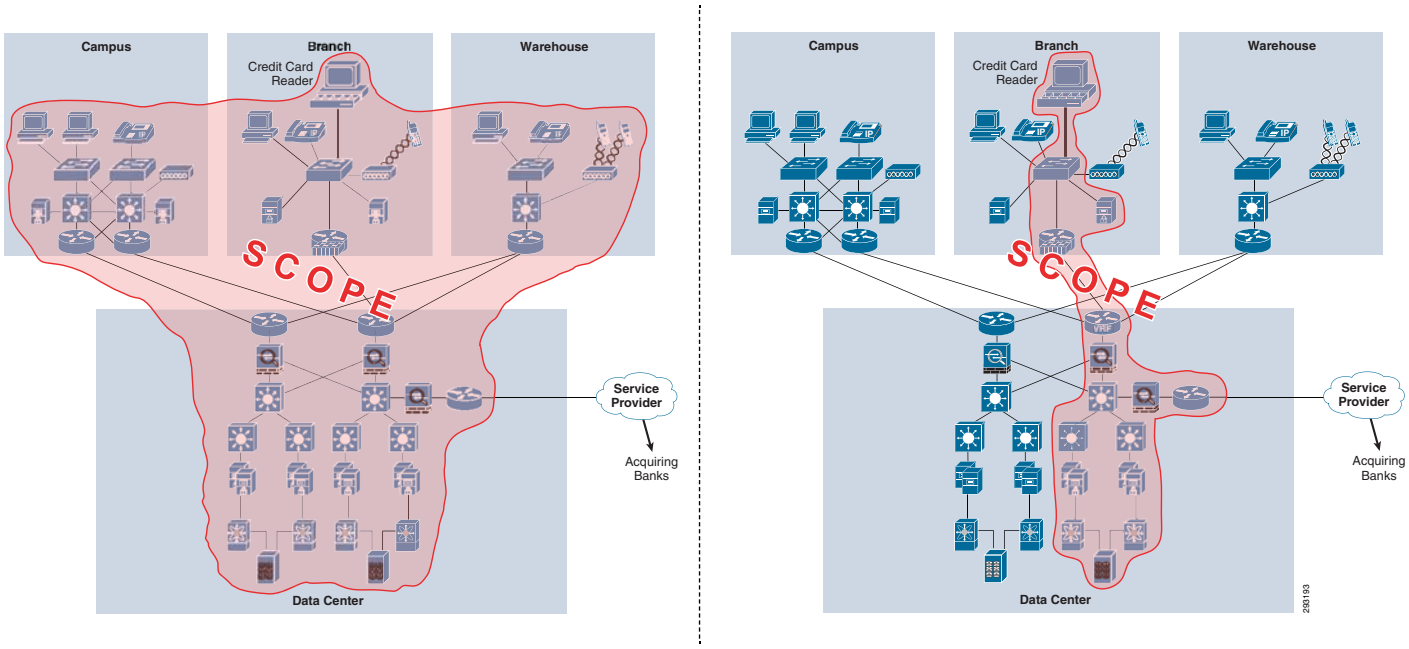
  With a clearly defined scope in which credit card data enters, flows, resides, and exits, you can easily identify the area's perimeter. Any boundary that touches public or untrusted networks must have firewall protection and intrusion detection capabilities.

- **Ensuring that you can effectively monitor the segmented environment**

  The Cisco Compliance Solution for PCI DSS 2.0 provides the ability to monitor the secured environment for threats, misconfiguration, and internal espionage. You must know the status of this sensitive area and the people that have access to it to maintain compliance.

Figure 1-2 shows an enterprise network that does not use segmentation and one that does.

Figure 1-2 Enterprise Architecture—Without and With Segmentation



The solution consists of strategic guidance as well as tactical implementation. Cisco is in the unique position to apply its enterprise-wide architecture experience to the requirements of PCI.

Chapter 3, "Solution Architecture," discusses what organizations should consider when designing their posture for addressing PCI. It examines enterprise architecture and discusses the related controls within them. Chapter 4, "Solution Implementation," provides specific design examples of these architectures, addressing PCI requirements using Cisco and partner technology. Chapter 5, "Component Assessment," then separates the solution architectures into their components. Each component is individually assessed for its capabilities, and configuration examples are given to demonstrate this utility. The solution shows how each component was assessed by Verizon Business and gives implementation examples and design considerations. Finally, Appendix C, "Verizon Business Reference Architecture Report—Cisco PCI Solution," is included. The solution is designed to conform to PCI DSS 2.0.

The solution was built and tested using a holistic enterprise perspective including the following:

- Endpoint considerations—Point-of-sale (POS) systems and payment devices, including wireless payment devices
- Administrative concerns within scope of PCI
- Cisco, RSA, EMC, VCE, and HyTrust network infrastructure
- Assessment by Verizon Business, a qualified security assessor

The result is a set of branch, data center, and Internet edge architectures and designs that simplify the process of becoming PCI compliant, maintaining that posture and providing the capability of awareness when under attack. The Cisco PCI solution is part of the Cisco SecureX strategy, which allows you to establish and enforce security policies across the entire distributed network, not just at a single point in the data stream. By leveraging global and local security intelligence for dynamic, real-time threat protection, Cisco SecureX responds to the evolving security needs of today's borderless network environments. More information about Cisco SecureX can be found at www.cisco.com/go/securex.

Target Market/Audience

This solution is targeted toward the following audiences:

- Technical or compliance-focused individuals seeking guidance on how to holistically design and configure for PCI compliance
- Organizations that require a qualified security assessor to provide a Report of Compliance
- Organizations interested in preparing for growth that will someday require a Report of Compliance.

Although all organizations that take credit cards are required to be PCI compliant, this solution is designed to help the larger companies simplify the complexity of compliance. Smaller companies can benefit from the design and guidance as well, but should consult their acquiring banks for specifics if they do not currently require an onsite audit. Specific card programs are available at the following locations to determine their specific categorization process;

- American Express—http://www.americanexpress.com/datasecurity
- Discover Financial Services—http://www.discovernetwork.com/fraudsecurity/disc.html
- JCB International—http://www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide—http://www.mastercard.com/sdp
- Visa, Inc.—http://www.visa.com/Cisp

Solution Benefits

This solution demonstrates how to design end-to-end systems that conform to PCI DSS 2.0 guidelines. Companies can simplify PCI compliance by building a similar network with the recommended configurations and best practices. In addition, this solution provides the following benefits:

- A reference set of architectural designs and the controls used to address PCI
- A detailed analysis of Cisco and Partner components and their relationship with PCI DSS sub-requirements
- A centralized management tool kit, which provides operational efficiency
- Insight into the PCI audit process by providing an assessment report from Verizon Business

PCI Solution Results

Table 1-1 provides a summary of the PCI assessment results.

Cisco Compliance Solution Components

This solution combines components to create an end-to-end solution conforming to the requirements of the PCI 2.0 guidelines. The result is a set of branch, data center, and Internet edge architectures and designs that simplify the process of achieving and maintaining compliance.

Endpoints	Primary PCI Function
Cisco IronPort Email Security	DLP
Cisco Physical Access Control	9.1
Cisco UCS and UCS Express	Servers
Cisco Unified CM and IP Phones	9.1.2
Cisco Video Surveillance	9.1.1

Administration	Primary PCI Function
Cisco ACS	7.1
Cisco Identity Services Engine	7.1, 11.1b, 11.1d
Cisco Prime LMS	1.2.2
Cisco Security Manager	1.2
Hytrust Appliance	10.5
RSA Authentication Manager	8.3
RSA Data Protection Manager	3.5
RSA enVision	10.5

Infrastructure	Primary PCI Function
Cisco ASA-Branch	1.3, 11.4
Cisco ASA-Data Center	1.3, 11.4
Cisco Branch Routers	1.3, 11.4
Cisco Branch Switches	Segmentation
Cisco Data Center Routers	1.2, 1.3
Cisco Data Center Switches	Segmentation
Cisco Data Center IDSM	11.4
Cisco MDS Switches	3.4
Cisco Nexus 1000V Series Switch	Segmentation
Cisco Nexus Data Center Switches	Segmentation
Cisco Nexus VSG	Virtual Firewall
Cisco Wireless	4.1, 11.1
EMC CLARiioN SAN	Storage

PCI Solution Results



CHAPTER 2

PCI and the Solution Framework

The PCI Data Security Standard (PCI DSS) provides guidance for securing payment card data. It includes a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS provides an actionable framework for developing a robust payment card data security process, including prevention, detection, and appropriate reaction to security incidents.

Table 2-1 lists the PCI DSS goals and requirements.

Table 2-1 PCI Data Security Standard (PCI DSS)

Goals	PCI DSS Requirements
Build and maintain a secure network	**1.** Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	**3.** Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	**5.** Use and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement strong access control measures	**7.** Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	**10.** Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an information security policy	**12.** Maintain a policy that addresses information security for all personnel

The PCI DSS standard uses these 12 tenets to define how companies should secure their systems, both technical and social.

PCI DSS 2.0—New Reporting Guidelines

PCI DSS 2.0—New Reporting Guidelines

With PCI DSS 2.0, more thorough evidence is required from the organization. This fact will not likely be called out anywhere within the PCI DSS 2.0 "Summary of Changes" document.

Historically, the PCI Security Standards Council (SSC) has provided qualified security assessors (QSAs) with a PCI "Scoring Matrix" document, which provides the validation and reporting requirements for each PCI DSS requirement. For example, one requirement may require the QSA to review a supporting document and process to confirm a requirement is in place, where another may require that a document (for example, a policy or procedure document) as well as configuration and/or system settings be examined.

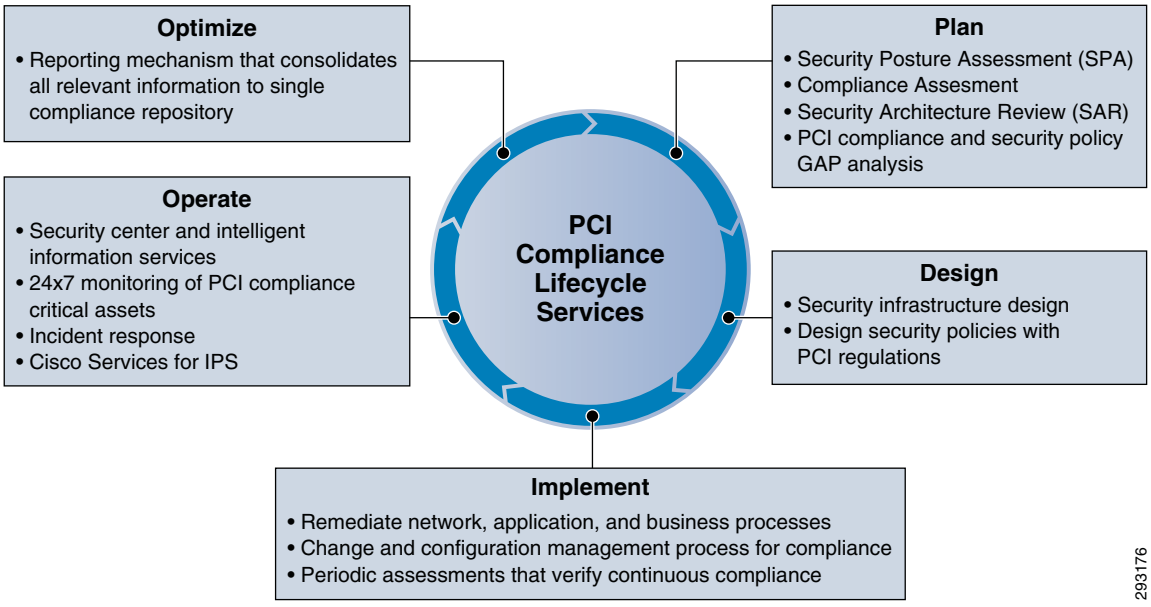
The Scoring Matrix has been replaced by a "Reporting Instructions" document. The necessary validation steps have been expanded. There is a greater level of detail required for assessor documentation (for example, observation of documentation, observation of process, action, or state, observation of configuration file/system settings, observation by interview, and so on).

These new instructions will likely lead to a more thoroughly conducted assessment.

Maintaining PCI Compliance

As stated in the overview, becoming compliant is not the real challenge associated with PCI. Although many companies view becoming compliant as a goal or an endpoint, it is better to view PCI as a continuous cycle rather than a snapshot in time (see Figure 2-1). This may seem intuitive, but many organizations relax after passing an audit. Rather than preparing for the ongoing activity of maintaining compliance, the posture that allowed the organization to pass degrades over time. Compliance is assumed to be continuous.

Figure 2-1 Continuous Compliance Cycle



A good model to adopt is one that looks at the full spectrum of time for maintaining and simplifying compliance:

- Future: Become compliant—What is the current state of the organization compared to the compliant state? What changes are needed to reach a state of compliance? Is there a new standard on the horizon or are there pending changes to the organization that might affect the state of compliance? Are there new location openings or mergers? What preparations are needed, both from a technical and process perspective, to account for maintaining compliance?
- Present: Know that you are still compliant—What tools are being used to recognize that the organization is in a state of compliance? Are there application dashboards that are succinctly developed to provide a current state of compliance? Is there a department or set of departments that "own" this state? Are there accurate diagrams and documentation for the full scope of the company that is within the scope of compliance?
- Past: What happened to the compliance?—Did someone in the organization turn rogue? Did someone from the outside break in? Did someone "fatfinger" a command? Who did? How can you account for what systems are in scope and gain forensic knowledge to account for who is doing what?

This solution is designed to provide the tools and design practices to help answer these questions.

Cardholder Data Environment and Scope

One of the most important concepts within PCI is the scope or the size of the organization's cardholder data environment (CDE). This is important for several reasons: the CDE comprises the specific applications, systems, and associated personnel that have access to sensitive data. This is the range of infrastructure and people that must successfully pass an audit to become PCI compliant. More importantly, this is also the area that must be properly maintained to be safe from the threat of a hacker. The term *sensitive data* refers to the items listed in Table 2-2, provided by the PCI DSS standard.

Table 2-2 Guidelines for Cardholder Data Elements

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	**Cardholder Data**	Primary account number (PAN)	Yes	Yes
		Cardholder name	Yes	No
		Service code	Yes	No
		Expiration date	Yes	No
	Sensitive Authentication Data	Full magnetic stripe data	No	Cannot store per Requirement 3.2
		CAV2/CVC2/ CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN block	No	Cannot store per Requirement 3.2

Wherever the data that corresponds to the fields in Table 2-2 are present in your organization, the appropriate measures must be taken to secure them.

PCI Best Practices

"Limit scope, protect it, maintain it…"

When it comes to simplifying PCI, this is probably the best advice:

> "Limit the size of the scope of your cardholder data environment, protect the area within the perimeter of that environment, and then strive to maintain it as efficiently as possible."

This guide demonstrates on many levels how pervasive this philosophy should be taken. *Limiting the scope* really means challenging your company. Challenge your management. Challenge the business. Challenge your department to weigh the risk versus the benefit of its current way of doing business. This does not necessarily mean that you must change. However, looking skeptically at the actual needs of the business combined with the sobering reality that there are organized criminals striving to steal from your company, you can systematically identify and document the true scope of your PCI environment and refine it to its core requirements. Minimizing the overall PCI scope and reducing unnecessary systems or unjustified access to systems reduces the ongoing requirements of PCI and simplifies the overall compliance cost and maintenance.

Several factors must be considered to maximize the efficacy of this philosophy. You must accurately determine the existing scope of what you have to secure before you can look at how to refine it. The following sections of this chapter discuss considerations of what might be in scope for your organization, and consequently your deployment using the Cisco solution framework for compliance.

The second part of the advice is to protect the area within the perimeter of the organization's scope. The majority of this manual gives guidance at varying levels of detail on how and where to implement controls for secure payment processing. Guidance is given from the architectural, design, and component perspectives to provide a comprehensive solution for protecting the cardholder data environment.

The final piece of the advice is to maintain it as efficiently as possible. The best way for organizations to ensure that this important aspect is not overlooked is to adjust their business processes to include a role within the organization that owns this responsibility. Many times, boards or representatives of different parts of the organization are brought together to develop a state of compliance. Without a clear owner of ultimate responsibility, organizations can sometimes suffer from diffusion of responsibility, and compliance can be lost within the cracks of silos of large organizations. By defining a person or group that identifies this as a chartered responsibility, organizations can ensure a focal point of identifying new risks as the organization changes over time.

Scope Maintenance

Documenting all known applications, their services, and systemic requirements from source to destination is required to fully understand the true range of the scope. This also provides a baseline to compare against for the ongoing requirement to ensure that scope does not unknowingly increase. This is also the area to apply that dose of skepticism. As the applications that are involved with payment card information are catalogued, determine whether any of the functionality can be maintained while removing sensitive data.

New PCI DSS 2.0 language has been added to clarify the organization's responsibility to discover and validate the PCI DSS scope within their environment, through a formally documented methodology.

From the PCI DSS 2.0 standard (page 10 under "Scope of Assessment for Compliance with PCI DSS Requirements"):

> *The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope. To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:*
>
> – *The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE).*
>
> – *Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).*
>
> – *The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE unless such data is deleted or migrated/consolidated into the currently defined CDE.*
>
> – *The entity retains documentation that shows how PCI DSS scope was confirmed and the results, for assessor review and/or for reference during the next annual PCI SCC scope confirmation activity.*

Changes to personnel, additions of new systems, addition of new branches, removal of obsolete accounts or systems, and anything else that affects the state of compliance should be exposed as a factor in an organization's compliance maintenance program. Monitoring which applications are accessing sensitive data and through which infrastructure systems must be updated on a regular basis. The PCI standard does not specify a method, so organizations can determine the best methods for their specific situations.

One option to comprehensively discover sensitive cardholder data is through the RSA Data Loss Prevention (DLP) Suite, which can accurately identify the location and flow of cardholder data throughout an environment. After files with sensitive information are identified and classified, they can be copied, moved, archived, deleted, or secured based on policy. The RSA DLP Suite is available in three modules:

- RSA DLP Datacenter can identify cardholder data and enforce policies across file shares, databases, storage systems (SAN/NAS), Microsoft SharePoint sites, and other data repositories.
- RSA DLP Network can identify cardholder data and enforce policies across corporate e-mail systems, web-based e-mail systems, instant messaging, and web-based protocols.
- RSA DLP Endpoint can identify cardholder data and enforce policies for such data stored or in use on laptops and desktops.

Each DLP module is centrally managed by the RSA DLP Enterprise Manager, a single browser-based management console. The RSA DLP Enterprise Manager offers dashboard, incident workflow, reporting, policy administration, and systems administration functionality.

Freeware applications such as the following can also be used to help document where your sensitive data resides:

- Spider
- SENF
- Snort
- Nessus

Scope Boundary Enforcement

Scope boundary and the relative security controls used to enforce it depend on the risk factors from the services that are present at that location. Table 2-3 summarizes the controls to use when various types of services are present at any location in the enterprise. The term "Location" refers to any place in the network such as a branch, a warehouse, campus or data center, for example.

Table 2-3 Location Services and Corresponding Compliance Controls

Location with Services	Minimum PCI Control Required	Relevant Solution Component
No point-of-sale (POS) located anywhere at location	No controls required	NA
Any POS location with systems	Rogue detection	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x switch
POS systems; no direct Internet access, no wireless access, no untrusted networks of any type	Segmentation requires minimum access control lists (ACLs); no state table required	Any router with ACLs
Basic wireless connectivity	Firewall, IDS to segment wireless from POS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS appliance
Wireless POS	Firewall, IDS, strong client encryption within wireless POS subnet	Cisco ISR, Cisco ASA, Cisco IPS appliance, Cisco Unified Wireless
Public WAN	Firewall, IDS	Cisco ISR, Cisco ASA, Cisco IPS appliance
Internet connectivity	Firewall, IDS	Cisco ISR, Cisco ASA, Cisco IPS appliance
Any untrusted network access	Firewall, IDS	Cisco ISR, Cisco ASA, Cisco IPS appliance

Cardholder Data Environment—Scope Layers

The following sections describe the three layers of the cardholder data environment.

Endpoints

Any endpoint or application that passes sensitive data needs to considered and secured from an end-to-end perspective. The following sections provide examples.

Point-of-Sale

Point-of-sale applications in the branch are the obvious candidates for documenting. Others include applications that access and use this sensitive information for other business processes. For example, customer relation management (CRM) applications are sometimes commingled with their customer's credit card data for customer data mining.

E-commerce and Public-facing Websites

Web applications continue to be a major point of entry for hackers. “SQL injections” are one method that hackers use to exploit poorly written front-end applications. E-commerce applications obviously need to be tested for vulnerabilities. However, *any* front-end web application should be treated with equal scrutiny. Some large breaches have occurred when a hacker was able to compromise a Human Resources website that accepted resumes. Defense in depth is needed across all perimeters, and any front-end application needs to have minimum standards.

Voice

Voice systems are not specifically called out in the standard. However, the standard is clear that entities must secure all systems that transmit cardholder data. Therefore, your entire voice system may be in scope depending on how sensitive data is being used. Are you taking phone payments? Are you recording sensitive data in a contact center? Are you using applications that take cardholder data over interactive voice response systems? Cisco phones have built-in Ethernet interfaces that can be used to connect to downstream registers. This saves wiring costs but puts the phone into scope, because it is now a system transmitting cardholder data.

Physical

Video surveillance systems that monitor the sensitive areas such as wiring closets within branches are considered to be part of the scope of compliance because they can document who had access to a sensitive physical area. Administrators of these systems are also considered to be in scope.

E-mail

Cisco does not recommend taking credit card payment information using e-mail. However, if this does occur, e-mail systems and clients would all be in scope.

Administration

Any piece of hardware that transmits sensitive data is considered to be in scope. Therefore, administration of those devices brings those administrative applications and administrators into scope.

People

Administrators who have access to the systems that process, transmit, or store sensitive data are also in scope. Strive to limit access to “business need-to-know” personnel. Clear role definitions can greatly reduce the population that can compromise your company by removing access for people that really do not require access to do their jobs. Approximately one-third of the breaches that occurred in 2009 were from internal personnel (2010 Verizon IBR). Restrict the administrative rights of your personnel to access systems that have sensitive data by allowing administrators privileges based only on the “need-to-know”. This can dramatically reduce the risk to your company and in event of a breach, reduce the range of candidates for a post-breach audit.

Processes

PCI compliance is typically not the only standard that must be addressed. Design your security policy to be as streamlined and efficient as possible while maintaining flexibility for other compliance regulations. Examples of common overlapping compliance standards include Sarbanes-Oxley or the Health Insurance Portability and Accountability Act (HIPAA). When developing an efficient holistic security policy, processes must be designed to minimize overall complexity for issues such as change control and administrative access and procedures.

Storage of Sensitive Information

Wherever sensitive information is stored, it must be encrypted. Storage area networks and in-branch processors are the main areas where encryption and key management procedures are applied. Virtual environments and cloud services should be heavily scrutinized for simplistic methods of compliance procedures.

Monitoring

Tools that provide the following monitoring capabilities are in scope:

- Real-time anomalous behavior
- Historical forensic analysis
- Configuration analysis to enforce template standards

Infrastructure

The physical infrastructure involved with the card data environment needs to be considered from an end-to-end perspective. Traditional components include firewalls, switches, routers, wireless access points, network appliances, and other security devices. Virtualization components such as virtual switches/routers, virtual appliances, and hypervisors that store, process, or transmit cardholder data are also in scope. Not all of the systems are obvious. Sometimes devices such as load balancers, WAN application acceleration devices, or content engines are overlooked and can be a source of compromise because these devices were not considered.

Architectural Sampling

One of the methods for reducing complexity is to standardize on architectures. For example, if you are able to replicate a standardized build across systems within the branch, auditors can take a sample of the total population of branches rather than having to audit every single branch. However, a common misperception is that only the branches that are audited are in scope. All branches are assumed to follow exactly the same build and procedures to use a sampling method. Be clear that in the event of a breach, a post audit will determine whether proper controls were applied across *all* branches. If this is found not to be the case, the organization may be liable for litigation.

Partners

Any business partner that connects to your network with access to sensitive data needs to be PCI compliant. There must be a signed agreement for culpability that designates responsibility and demarcation between the two companies.

Service Providers

Any service provider that connects to your network with access to sensitive data should be PCI compliant. There must be a signed agreement for culpability that designates responsibility and demarcation between the two companies.

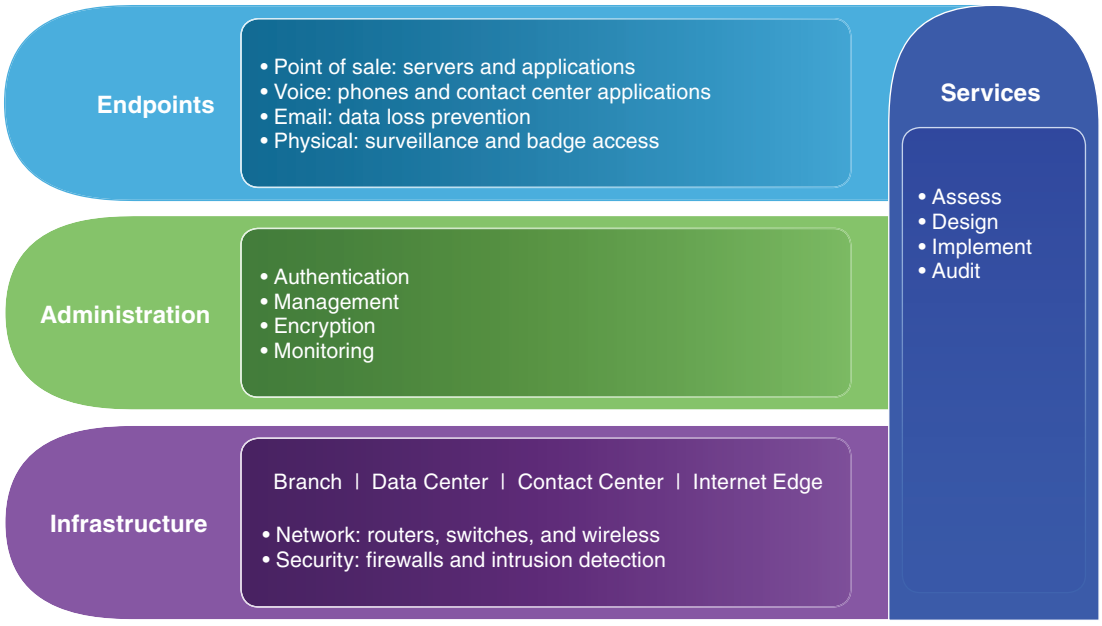
Internet

The Internet is a large public network that introduces a host of threats. Wherever direct Internet access is available, it should be considered a perimeter requiring a firewall and IDS/IPS technology to secure that access.

PCI Solution Framework

Figure 2-2 shows a comprehensive view of the elements previously discussed, and shows how the Cisco Compliance Solution for PCI organizes them into a solution framework. By using this framework, PCI can be simplified into three overarching layers that provide a simple way to discuss the complexity of the topic.

Figure 2-2 Cisco PCI Solution Framework



The Cisco PCI solution framework is used throughout this guide as a model.

Endpoints

This layer of the solution takes into account any application or endpoint that is involved in the scope of a PCI audit. An application is defined as any that uses cardholder data *or* is not segmented away from the cardholder data environment (CDE). Examples of an endpoint include a point-of-sale (POS) server, POS register, surveillance camera, wireless line buster, and so on.

Administration

This layer of the solution addresses areas of PCI compliance that affect the CDE at an administrative layer. It is defined by how systems are accessed (management and authentication), where sensitive data resides or is stored (encryption), and how alerts to this environment are used (monitoring).

Infrastructure

This layer of the solution framework addresses the infrastructure components such as routers, switches, firewalls, and security components.

Services

Services for designing, implementing, and auditing can be found from both Cisco and Verizon Business at the following URLs:

- Cisco—http://www.cisco.com/en/US/products/svcs/services_area_root.html
- Verizon—http://www.verizonbusiness.com/Products/security/

Services for maintaining vulnerabilities:

- Intellishield Alert Manager—The Cisco Security IntelliShield Alert Manager Service is a web-based, security alerting service that proactively notifies customers about emerging information security-related threats and vulnerabilities. The service also includes features that help customers securely manage risks and vulnerabilities within the customer's organization, such as the ability to manage workflow and track remediation efforts.

The IntelliShield Alert Manager service includes the following:

- Vulnerability alerts
- Malicious code alerts
- Threat outbreak alerts
- Applied mitigation bulletins
- Cyber risk reports

For more details on the IntelliShield Alert Manager service, see the specific service description at http://www.cisco.com/go/servicedescriptions/.



CHAPTER 3

Solution Architecture

The Cisco PCI solution is a set of architectures, strategic principles, and tactical designs that details a holistic approach to addressing the requirements of PCI DSS 2.0. The Cisco enterprise architecture is used as a baseline for demonstrating the range of places that typically exist within an enterprise. This chapter describes the Cisco enterprise architecture in detail, so that when the discussion of specific PCI controls is discussed, the controls can be placed in context with that enterprise-wide view. The solution looks at an enterprise from an end-to-end perspective; from the branch, where someone swipes the credit card, to the back-end of the data center, where the transaction leaves the organization's network to be processed by the acquiring bank.

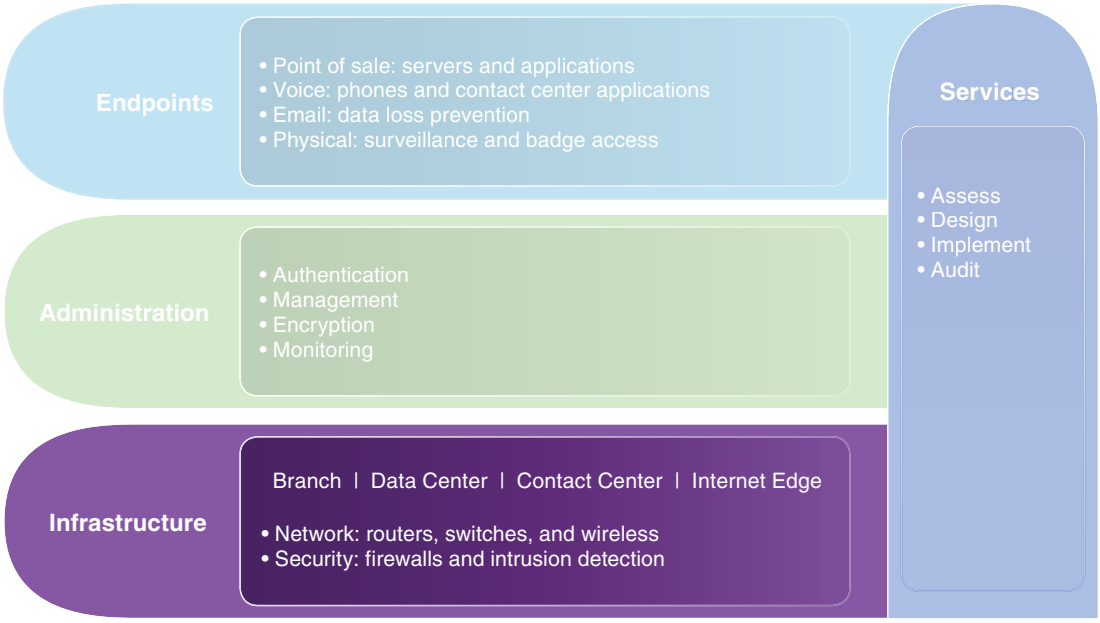
For specific designs referencing these architectures, see Chapter 4, "Solution Implementation."

For more information on the individual components used to build these architectures, see Chapter 5, "Component Assessment."

Chapter 2, "PCI and the Solution Framework," describes the elements that make up the solution framework. The solution framework organizes the scope of the cardholder data environment for contextual reference. The bottom layer of the model shows the organization of the enterprise into places such as the branch, data center, and the Internet edge. (See Figure 3-1.)

Enterprise Architecture and PCI Design Considerations

Figure 3-1 Solution Framework

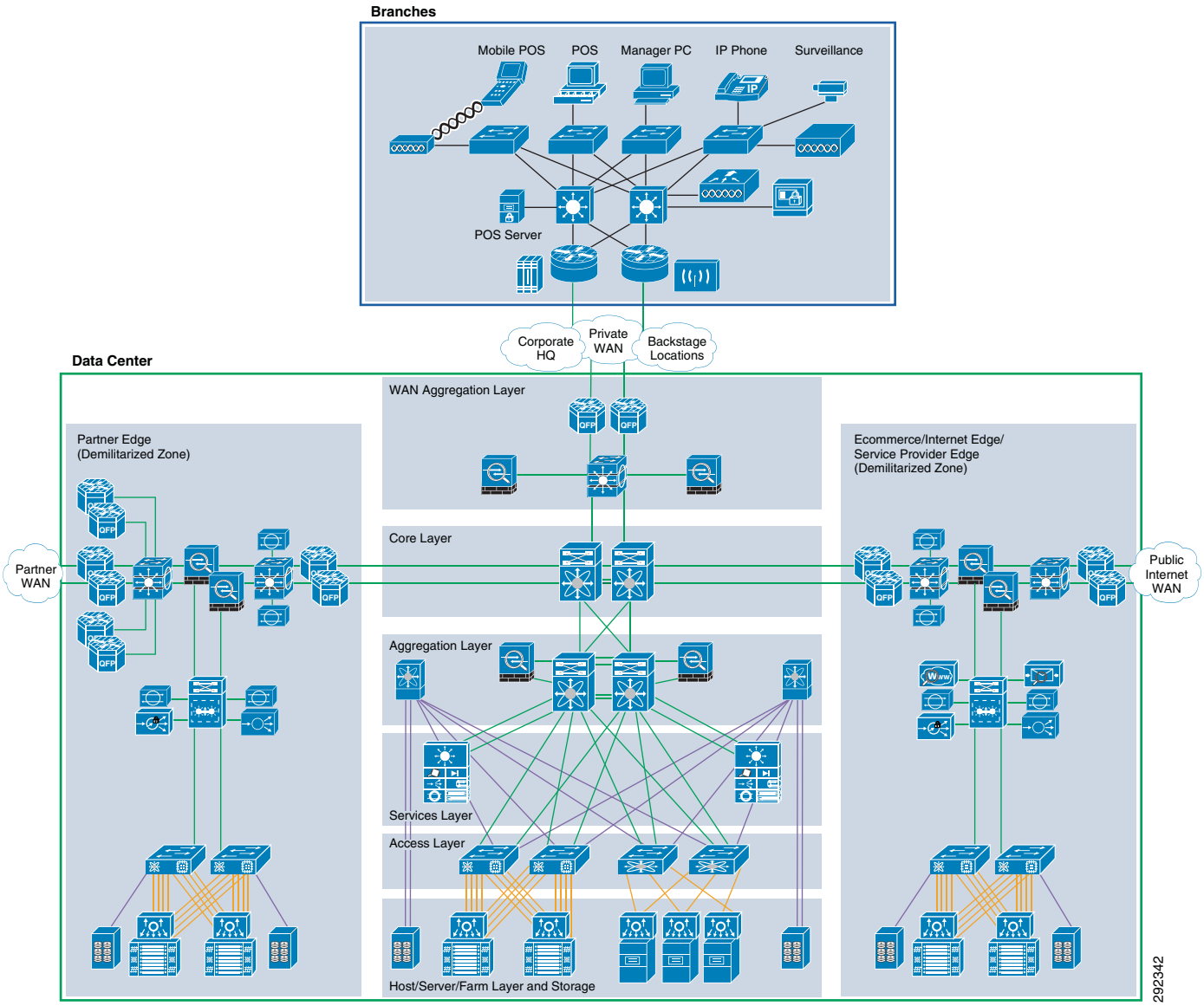


Enterprise Architecture and PCI Design Considerations

PCI compliance affects the overall enterprise architecture, depending on the requirements of the business. For example, a new business requirement for direct customer Internet connectivity at the branch level extends the firewall and IDS/IPS perimeter requirements to the branch level, whereas before it might exist only at the headend data center. Without this contextual reference, it is difficult to discuss specific controls.

Figure 3-2 shows the enterprise-wide reference architecture and locations that commonly exist in an organization's domain.

Figure 3-2 Enterprise-wide Reference Architecture



Enterprise Network Addressing

Segmentation partitions sensitive data from non-sensitive data. By separating sensitive information from normal information, you are able to treat it differently. Enterprise addressing plans should take this into account by separating compliance data onto its own set of addresses. Whether in the data center or in the branch, by having compliance data use its own addressing plan, you are able to enforce its boundaries with the required controls depending on the contextual risk.

Design Considerations

Within the Branch

Branch addressing should have a separate network for payment involved applications and equipment. This should be separated from normal data, wireless data, wired/wireless guest and other compliance data.

See Branches, page 4-4 for configuration examples.

Within the Data Center/Internet Edge

PCI DSS Sub-requirement 1.3.8 states: “Do not disclose private IP addresses and routing information to unauthorized parties.” This aligns with the defense-in-depth strategy. By obfuscating internal addressing schemes to the public, especially addresses that could be attacked with payment card information, you reduce your attack surface.

Regardless of the IP version that an enterprise uses (IPv4 or IPv6), methods must be used that eliminate the visibility of the internal addressing scheme. Proxy, NAT, route filtering, and other methods achieve this. Since the World IPv6 Launch of 2012, IPv6 is becoming more commonly deployed within enterprise merchants and service provider offerings. However, not all vendor technology necessarily supports IPv6. so compliance consideration must be given when deploying it.

See Internet Edge Design, page 4-23 for a configuration example.

The following sections describe the major places affected by PCI compliance throughout the enterprise. Each section provides design considerations that are affected by PCI controls in more detail.

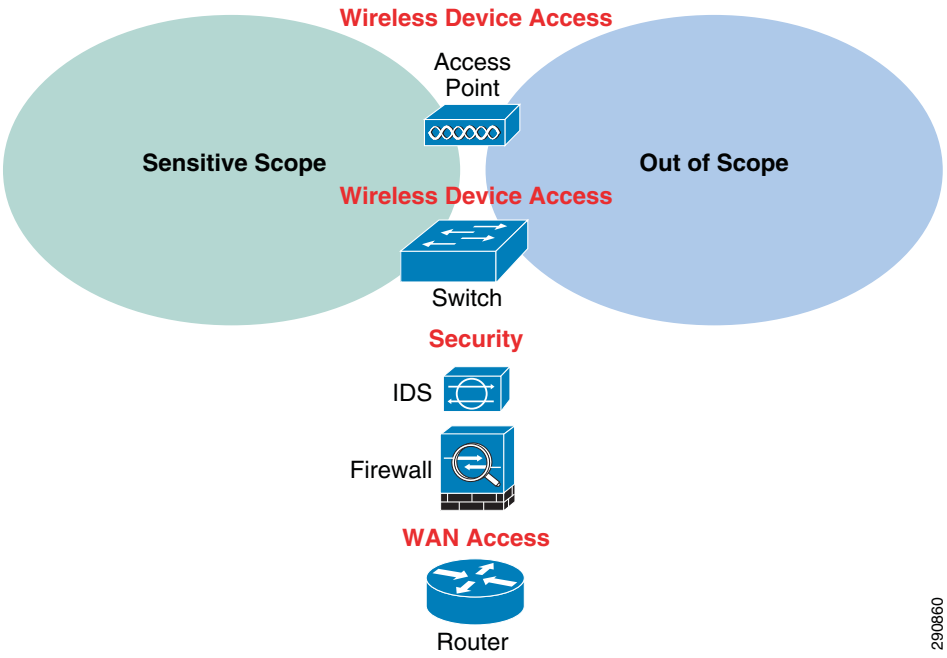
Branch Architecture

The branch is the location where customers swipe their credit cards to purchase goods. Depending on the type of services that are offered at the branch, various levels of security are required. This section discusses those design considerations and relates them to various branch formats.

Design Considerations

Figure 3-3 shows the fundamental infrastructure components used within a branch location. These components are used in conjunction with each other to segment sensitive data from non-sensitive data. The process of segmenting the network into *scopes* allows an organization to reduce the amount of branch-level components that need to be audited. Note that devices/endpoints themselves may be cut out of the scope of an audit by putting them onto their own network, but the actual network infrastructure may not necessarily be decreased. For example, a switch can have devices that are both sensitive and non-sensitive attached to it. By putting the non-sensitive devices onto their own VLANs, they can be cut out of the audit by using the VLAN function of the switch. However, the switch itself still remains in scope.

Figure 3-3 Fundamental Branch Infrastructure Components



Each branch component is used for a different function, as follows:

- The router function can be used for:
  - Accessing the WAN
  - Routing between VLANs
  - Access control lists
- The firewall can be used for:
  - Filtering unnecessary or inappropriate data via a stateful firewall
  - Routing between VLANs
  - Detecting and preventing intrusions; (IPS/IDS devices can also be separate appliances)
- Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS) monitor for anomalous behavior on the network and send alerts.
- The switch can be used for:
  - Segmenting via VLANs
  - Accessing wired devices
- The access point can be used for:
  - Wireless segmentation
  - Accessing wireless devices

The function of each of these devices can be virtualized and consolidated for simplicity, depending on the space and management requirements of the branch footprint. For example, some smaller branches have power, wiring closet, rack, and cabling restraints that would benefit from virtualized devices that reduce the physical footprint of the branch infrastructure.

Conversely, each of these devices can be increased in number depending on the resiliency and redundancy requirements of the business. For example, if branch connectivity is a business priority, using redundant routers for redundant WAN access might be a requirement to ensure that branch connectivity is maintained.

Regardless of how the branch is designed from a redundancy or scale perspective, the same types/locations of controls are consistent across them.

Many organizations use their data center as their centralized location to connect to public networks such as the Internet. This perimeter is typically secured as a demilitarized zone (DMZ) using firewalls and IDS/IPS. Whenever you introduce any type of untrusted network (wireless, Internet, microwave, satellite, cellular, and so on) into the branch environment, you have effectively created a new external perimeter that must now be secured with a firewall and intrusion detection/prevention system. Table 3-1 defines the types of factors that affect branch controls and requirements.

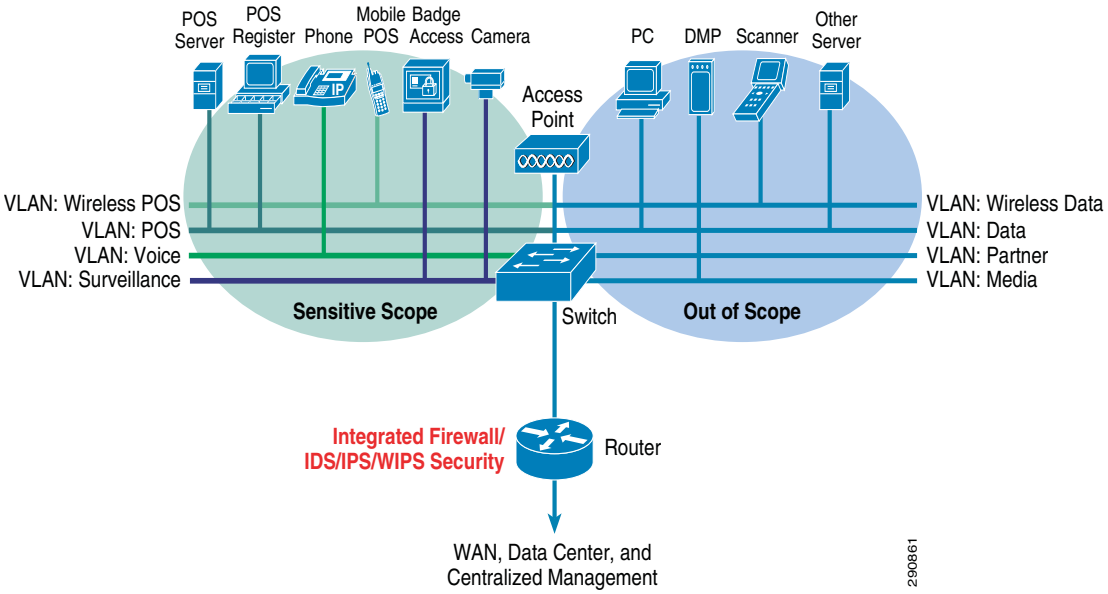
Table 3-1 Branch Services and Corresponding Compliance Controls Located at Branch

Branch Service Type	Minimum PCI Control Required	Relevant Solution Component
Any branch with point-of-sale (POS) systems	Rogue detection	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x switch
POS systems; no direct Internet access, no wireless access, no untrusted networks of any type	Access control lists (ACLs), no state table required	Any router with ACLs
Basic wireless connectivity	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS appliance
Wireless POS	Firewall, IDS, strong client encryption	Cisco ISR, Cisco ASA, Cisco IPS appliance, Cisco Unified Wireless
Public WAN	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS appliance
Internet connectivity	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS appliance
Any untrusted network access	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS appliance

The fundamental reference branch architecture assumes that an organization may eventually need to scale to these levels of services, but not necessarily immediately. From a branch perspective, the Cisco Integrated Services Router (ISR) performs each of the functions listed in Table 3-1. This allows organizations to grow with their investment by purchasing a router that can scale by different license keys for different services without having to rip and replace. For example, a business can purchase a Cisco ISR for basic WAN connectivity. When the business wants to introduce wireless to the branches, the business can then unlock the firewall/IPS/IDS feature set with a license.

The fundamental branch reference architecture in Figure 3-4 shows the solution framework endpoints/applications within the context of the fundamental branch component's infrastructure.

Figure 3-4 Fundamental Reference Architecture



In-scope devices can include the following:

- POS devices
- Wireless handheld devices
- Mobile POS
- Voice systems
- Physical badge access
- Video surveillance systems.

In general, an additional VLAN for management of infrastructure should be distinctly defined.

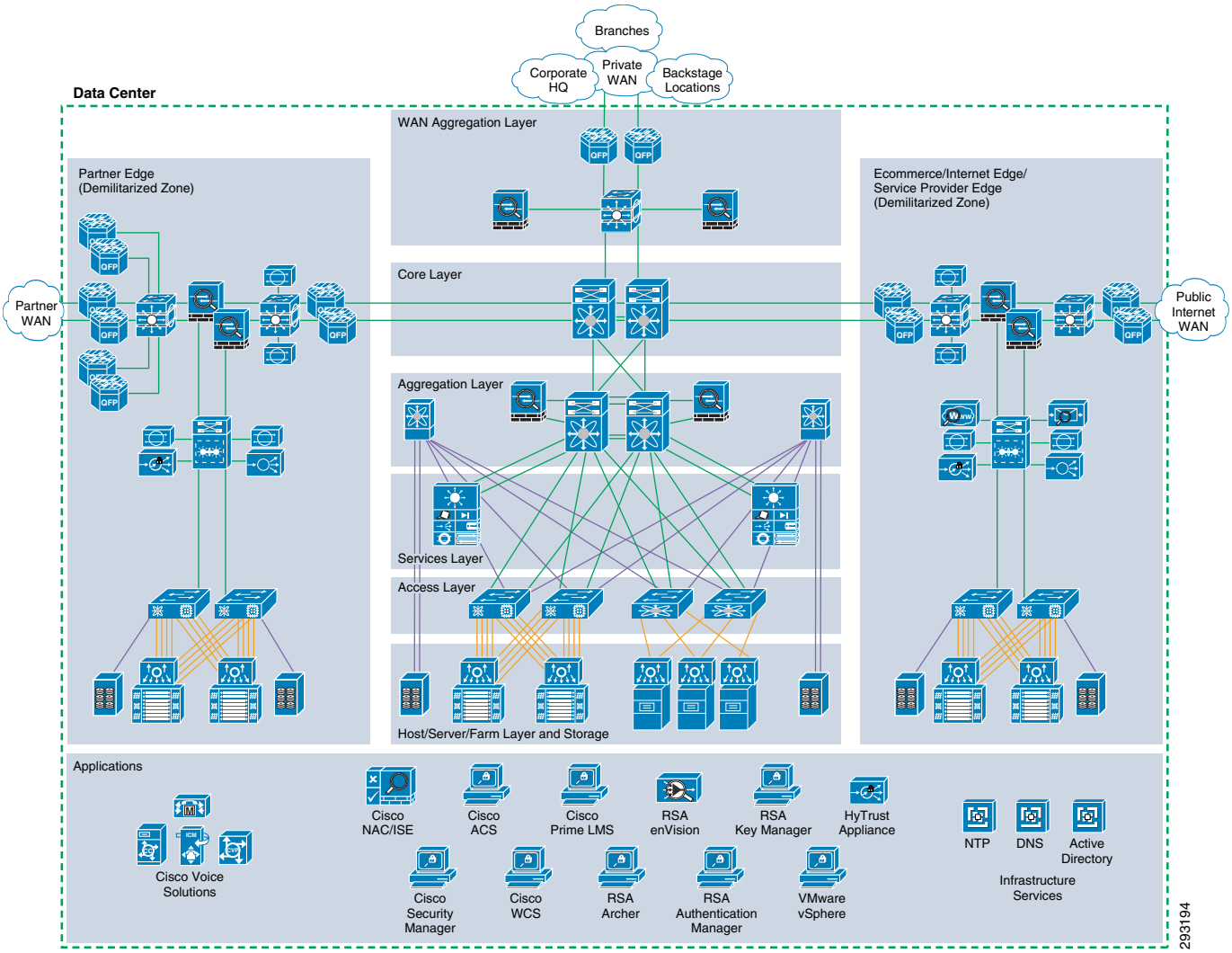
The remaining devices at the branch level are considered *out-of-scope* and do not need to be audited, given that they are on their own network and segmented via firewall/IPS/IDS from the sensitive networks.

The PCI branch model and its controls were applied to the small, medium, and large branch footprints and are shown in Chapter 4, "Solution Implementation," in detail. This section provides sample addressing plans used by various branches. Many designs can be extracted by understanding and using the PCI solution model shown above, but the overall functions are essentially the same.

Data Center

The data center is where centralized data processing, data storage, and data communications take place (see Figure 3-5). The data center is also the place where management systems are deployed. The data center provides centralized control from an administrative perspective because it is typically where the tools that are used to monitor and enforce compliance are deployed.

Figure 3-5 Data Center Architecture



Design Considerations

Design considerations are as follows:

- Centralized solution management that supports all aspects of network, security, and systems management; and supports remote access from anywhere on the network.
- Standardized equipment and software images, deployed in a modular, layered approach, that simplify configuration management and increase the availability of the system.
- A highly available data center design that permits highly resilient access from branches to core data and storage services.
- WAN aggregation alternatives that allow flexible selection of service provider network offerings.
- A service aggregation design that allows for a modular approach to adding new access layers and managing shared network services (for example, firewall, IDS, application networking, wireless management).

- Firewall, IDS, and application networking services that are available at the service and aggregation layers of the data center.
- Scalability that can accommodate shifting requirements in data center compute and storage requirements.
- Note that WAN access speeds are typically the limiting factor between the branch network systems and the WAN aggregation layer. It is typical for organizations to over-subscribe the WAN circuits between the branches and the WAN edge aggregation router. Over-subscription can cause inconsistent results and packet loss of payment card information in the event that more traffic enters the WAN circuit simultaneously.
- Backup network connections from branch networks to the data center are recommended when payment card information is transported via the WAN.

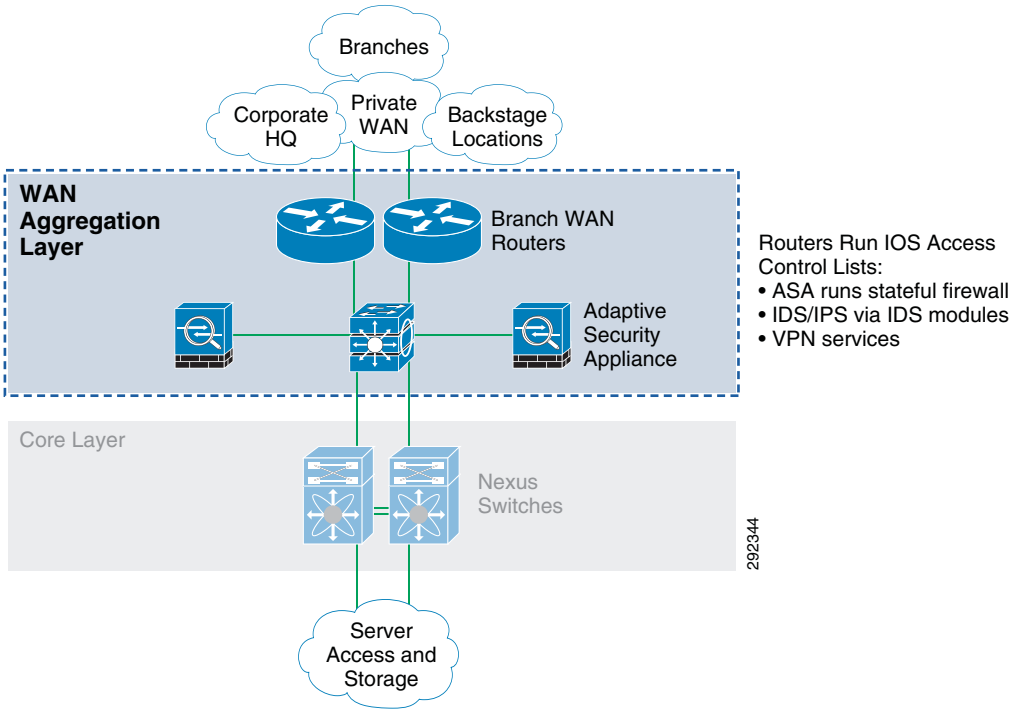
Data centers can house many types of functions, and the term itself can encompass narrow and broad aspects. For the purposes of this guide, data centers include the following functions:

- WAN aggregation layer—Aggregates the branch and backstage WAN connections to the core
- Core layer—Highly available, high-speed area that is the central point of connectivity to all data center areas
- Aggregation layer—Aggregates the services of one area and connects that area to the core
- Services layer—Data treatment and manipulation occurs between the access layer and aggregation layer
- Access layer—Server-level access and connectivity between hosts/servers to the services and aggregation layers, depending on the nature of the application
- Host/server farm—Physical servers, virtualized servers, and appliances' host applications
- Storage—Storage area networks (SANs)
- E-commerce—Internet-based transactions
- Internet/service provider edge demilitarized zone (DMZ)—Secure connectivity to the Internet
- Partner edge DMZ—Secure segmented connectivity to partners

WAN Aggregation

The WAN aggregation layer is a transit network that aggregates the connections from the branches, backstage locations, and corporate offices, as shown in Figure 3-6.

Figure 3-6 WAN Aggregation Layer



Design Considerations

The WAN edge routers should not also be used as the Internet gateways for the data center network. By clearly defining zones of separation of responsibility within the infrastructure, it is easier to maintain.

Two options are possible at this layer for Layer 3 filters at the WAN aggregation layer:

- Firewall appliance—Interior to the WAN edge routers, a dedicated firewall appliance is used to secure incoming WAN traffic and to terminate branch VPN connections. This design provides the highest scalability.
- Cisco IOS Software firewall routers—Many Cisco routers also support the Cisco IOS Security Software option that includes a firewall feature. Cisco recommends the use of the Cisco IOS Security feature set in branches and teleworker deployments, because of a much lower number of users and connection rates than at the branch WAN aggregation headend location.

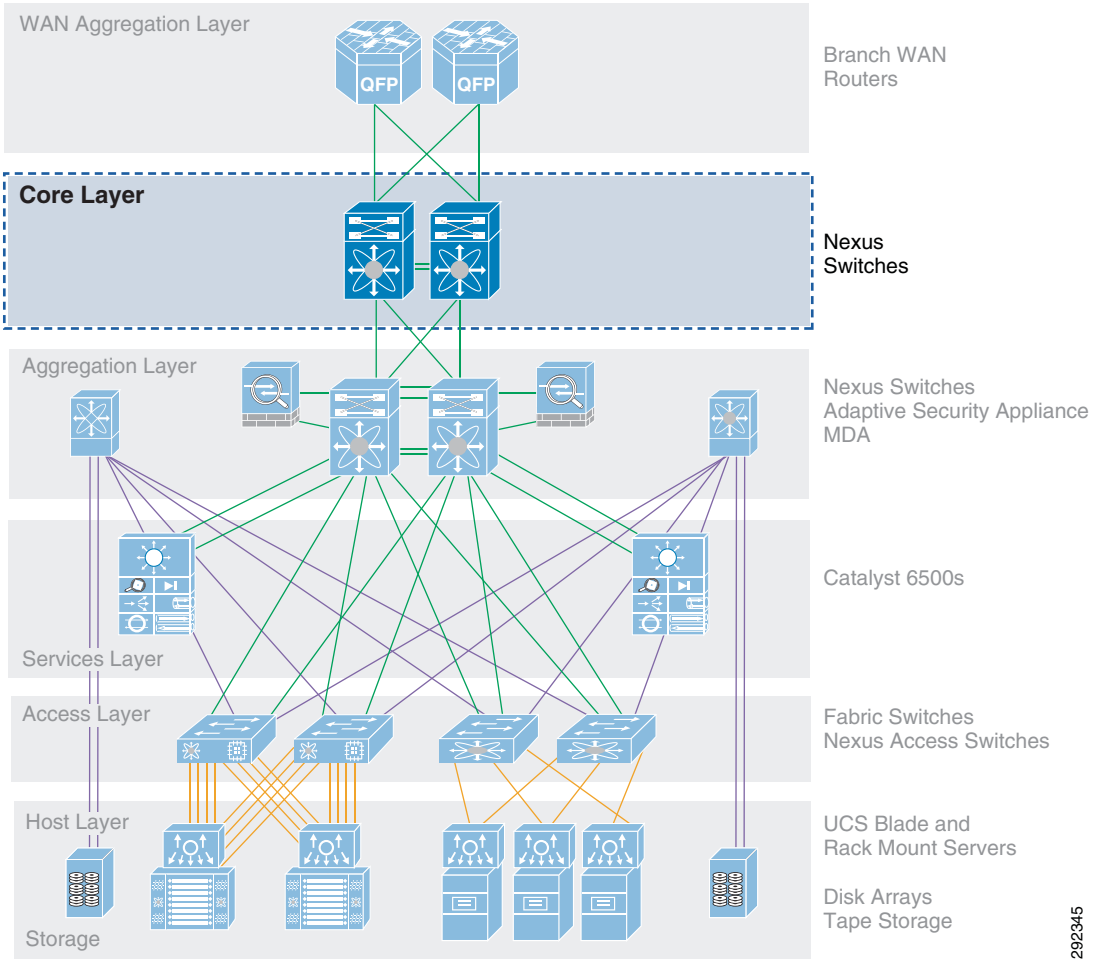
There are two typical WAN speeds categories for a WAN aggregation network: less than and up to OC3 (155 Mbps), and OC12 (622 Mbps) and above. The choice of these two network speeds determines the platform set to select from Cisco. In addition, this design creates two profiles for each WAN speed. These profiles are designed to provide guidance when designing a WAN edge network, regardless of which enterprise WAN architecture is selected. The profiles for each WAN speed investigate integrated versus dedicated chassis for each functionality component, as highlighted in the previous section. Some customers prefer a highly integrated solution where most, if not all, of the WAN edge functions described in this document reside on a single or very few network devices. Other customers prefer the granularity and scalability of these same functions separated across multiple network devices.

The WAN aggregation architecture is based on the *Infrastructure Protection and Security Service Integration Design for the Next Generation WAN Edge v 2.0*, which can be found at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/IPSNGWAN.html

Core Layer

The core layer provides the high-speed packet switching backplane for all flows going throughout of the data center, as shown in Figure 3-7.

Figure 3-7 Core Layer



Design Considerations

The core layer provides connectivity to multiple aggregation layers and provides a resilient Layer 3 routed fabric with no single point of failure. The core layer runs an interior routing protocol, such as Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), and load balances traffic between the core and aggregation layers using the Cisco Express Forwarding-based hashing algorithms.

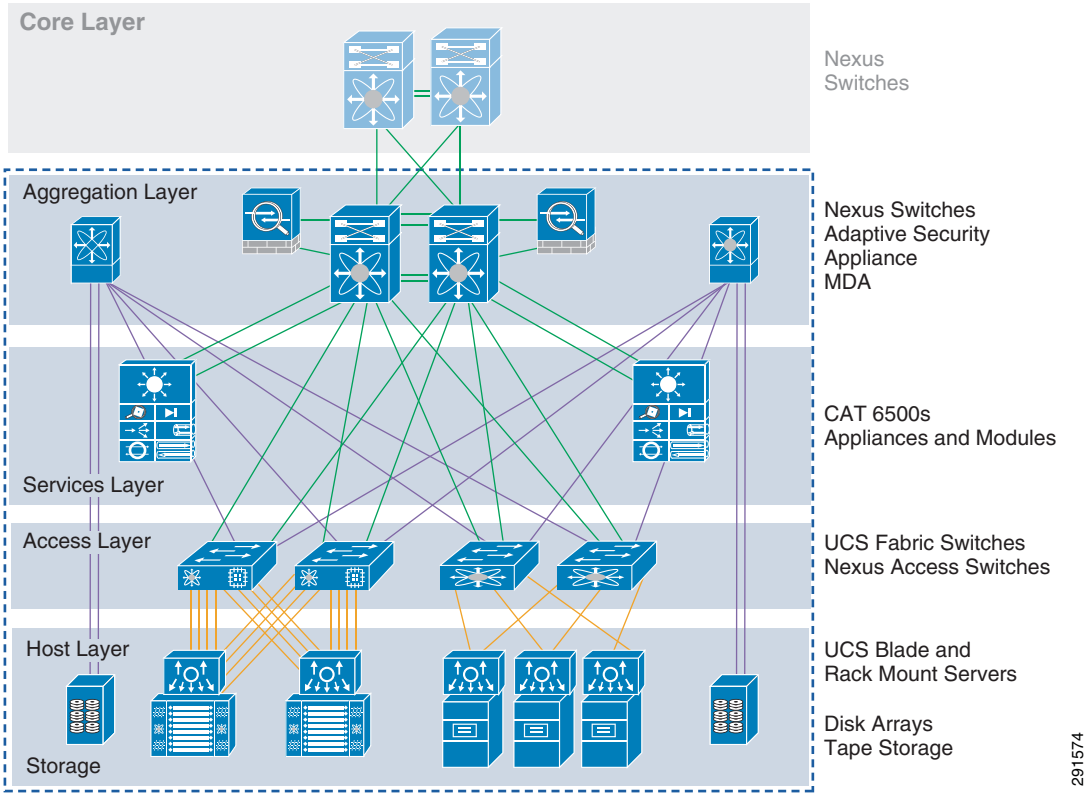
The core is not a perimeter; no security filtration should be performed at this layer.

The core, services aggregation, and server access tiers of the multi-tier data center architecture were based on the design documented in the *Cisco Data Center Infrastructure Design Guide 3.0*, which can be found at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/DC-3_0_IPInfra.html

Aggregation Block

An aggregation block is a combination of the aggregation, services, and access layer systems. It represents a repeatable, implementable template for scaling applications and services within the data center. (See Figure 3-8.)

Figure 3-8 Aggregation Block



Design Considerations

Zones are a best practice to isolate applications and services based on their individual policy requirements. You can securely mix in-scope and out-of-scope applications and services within a single aggregation block.

The layers that comprise the aggregation block are described in more detail below.

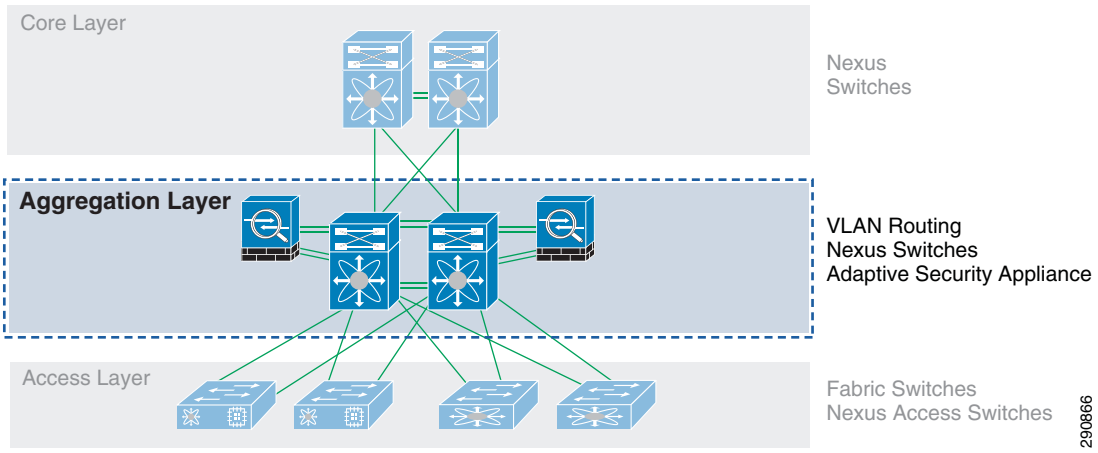
For more information, see the following URLs:

- http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_2.html
- http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/nx_7000_dc.html

Aggregation Layer

The aggregation layer aggregates the connections from the services layer and the access layer to the centralized core, as shown in Figure 3-9.

Figure 3-9 Aggregation Layer



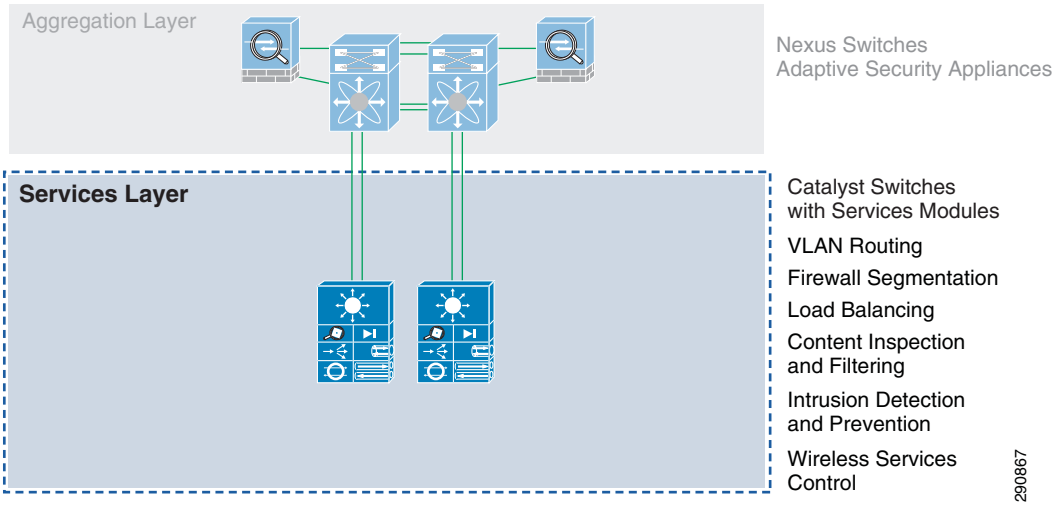
Design Considerations

The aggregation layer uses Layer 3 filters to segregate and protect the edge of the scope of compliance.

Services Layer

The services layer provides important functions, such as service module integration, Layer 2 domain definitions, spanning tree processing, and default gateway redundancy. (See Figure 3-10.)

Figure 3-10 Services Layer



Design Considerations

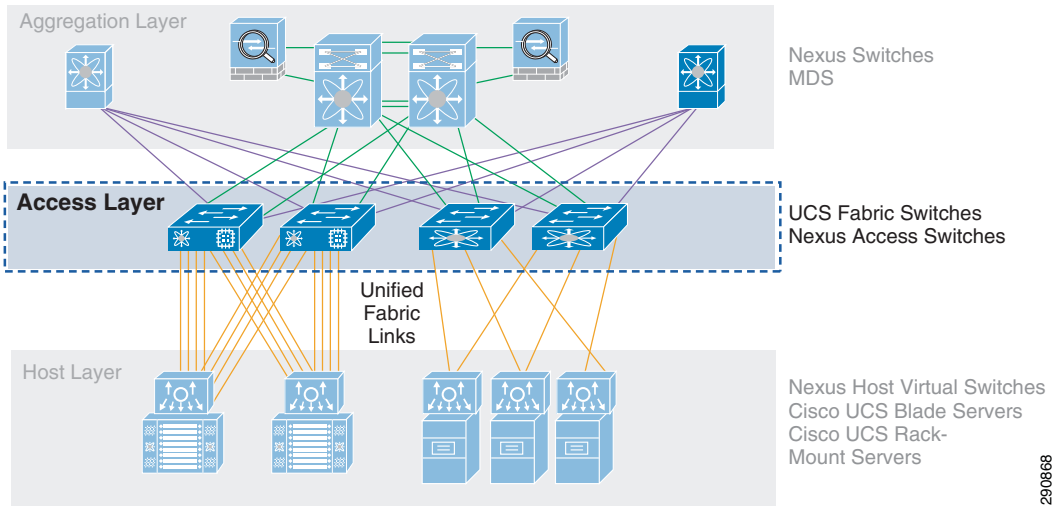
Services such as server load balancing and wide-area application services (WAAS) are used at this layer to optimize applications. Optimizing devices used within the scope of PCI are also brought into scope and are susceptible to the same controls as traditional network devices. For more information on understanding these controls, consult the capability assessment logic in Chapter 5, "Component Assessment."

Services such as content switching, SSL offload, intrusion detection, and network analysis are provided by hardware-based service modules or standalone appliances.

Access Layer

The access layer is where the servers physically attach to the network, as shown in Figure 3-11.

Figure 3-11 Access Layer



In typical data centers, the server components consist of appliances, 1RU servers, blade servers with integral switches, blade servers with pass-through cabling, clustered servers, and mainframes with OSA adapters. The access layer network infrastructure consists of modular switches, fixed configuration 1RU or 2RU switches, and integral blade server switches.

Design Considerations

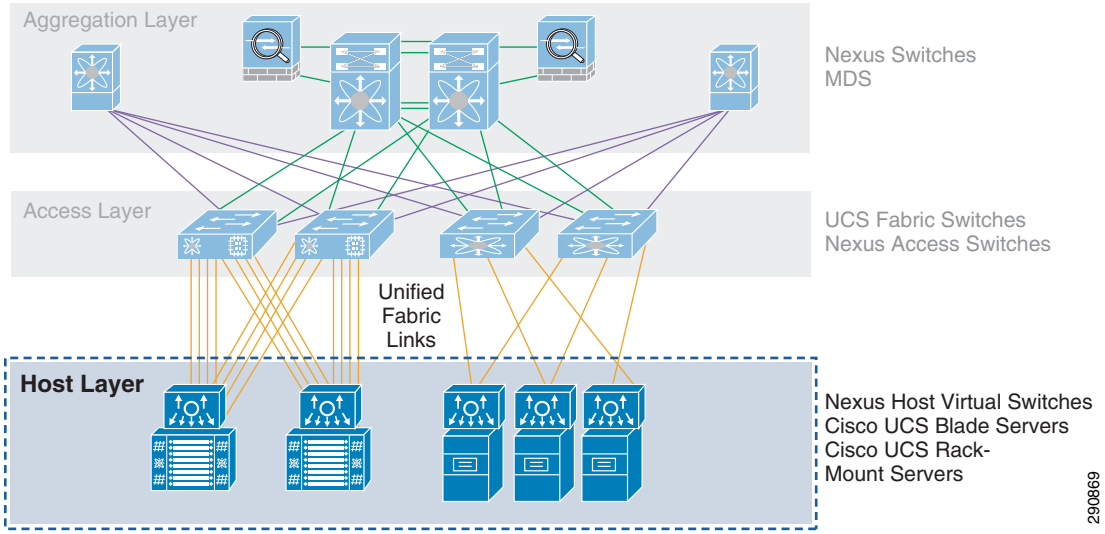
Switches provide both Layer 2 and Layer 3 topologies, fulfilling the various server broadcast domain or administrative requirements.

The solution management servers connect to the network in this layer. They are centralized, segmented from other business application servers, and protected by firewall services from the service aggregation layer above. Business servers, consisting of POS transaction log servers, database, and data warehouse servers also exist at this layer but are segmented via separate VLANs and firewall policy.

Host/Server Farm Layer

The host/server farm layer is where the centralized administrative applications reside, as shown in Figure 3-12.

Figure 3-12 Host/Server Farm Layer



Design Considerations

Network addressing should be used per business function. This allows the discrete manipulation of data traffic as requirements arise. For example, both POS applications and network management are used within the scope of PCI compliance but should be segregated onto their own subnets.

Virtualization technology can be used within a data center server farm. Individual blades within a blade server chassis can be used to segment sensitive and non-sensitive applications because they run independent hypervisors. Because hypervisors are considered insecure, when mixing sensitive applications with non-sensitive applications (mixed-mode) across the same hypervisor, the non-sensitive applications are now in scope.

For more information, see the PCI Virtualization Guidelines whitepaper at the following URL: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.

Multiple internal Network Time Protocol (NTP) servers should be deployed for consistent log synchronization in the event of failure. Those internal NTP servers should use more than one external source in the event of an external failure.

Although virtualization can be used for a variety of services, NTP requires a high resolution system clock and accurate response times to clock interrupts that virtual machines cannot provide. For these reasons, it is recommended not to run NTP on virtual machines. Instead, NTP should be run on the base OS of the hypervisor, and the virtual machine should use VMware Tools Clock synchronization to sync with the base host. NTP servers should also not run on virtual machines but on physical devices (for example, on the Cisco Catalyst 6509 Services switches in the services layer of the data center aggregation block). For more details, see the following URL: http://www.vmware.com/files/pdf/Timekeeping-In-VirtualMachines.pdf.

Table 3-2 lists descriptions of applications for administrators.

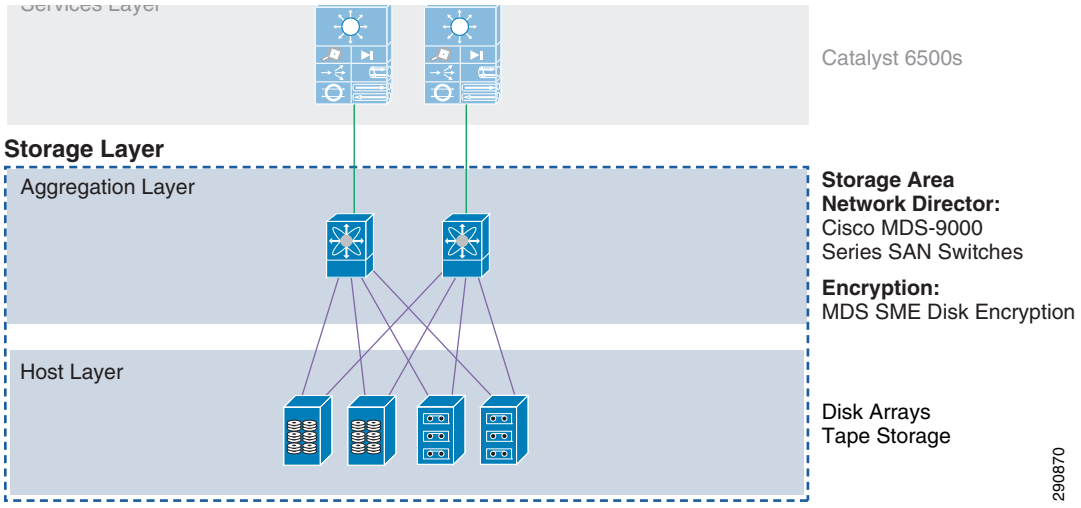
Table 3-2 Central Toolkit Description of Applications for Administrators

Function	Solution Component Options
Authentication	
Device AAA	Cisco Secure ACS, Cisco ISE
Two-factor remote	RSA Authentication Manager
Directory services	Active Directory
Network Management	
Device configuration	Cisco LMS
Security configuration	Cisco Security Manager
Wireless configuration	Cisco WCS
Monitoring	
Event correlation	RSA enVision
Policy enforcement	Cisco LMS
Corporate policy	RSA Archer
Virtualization	EMC Unified Infrastructure Manager, VMware vSphere
Physical Security	
Video surveillance	Cisco Video Surveillance Manager
Building access	Cisco Physical Access Manager
Encryption	
Storage	Cisco Key Manager, RSA Data Protection Manager
Remote access/VPN	Cisco Security Manager

Storage Layer

The storage layer is where sensitive data is stored, as shown in Figure 3-13.

Figure 3-13 Storage Layer



Design Considerations

A combination of disk encryption provided by Cisco MDS, Fibre-Channel zoning, and masking were used in the storage implementation of this solution. By deploying zoning within a Fibre Channel fabric, device access is limited to devices within the zone. This allows the user to segregate devices based on access to a particular storage device (disk array). This is a requirement in a data center environment in which multiple file servers in the data center server farm are connected to the same SAN fabric, and access to cardholder data must be restricted to a subset of servers. LUN masking takes zoning beyond the Fibre Channel switchport level, by restricting access to specific LUNs on a given disk array. Only specific devices belonging to the LUN zone are able to access those sections of the disk.

Encryption keys for storage are managed by Cisco Key Manager and RSA Data Protection Manager.

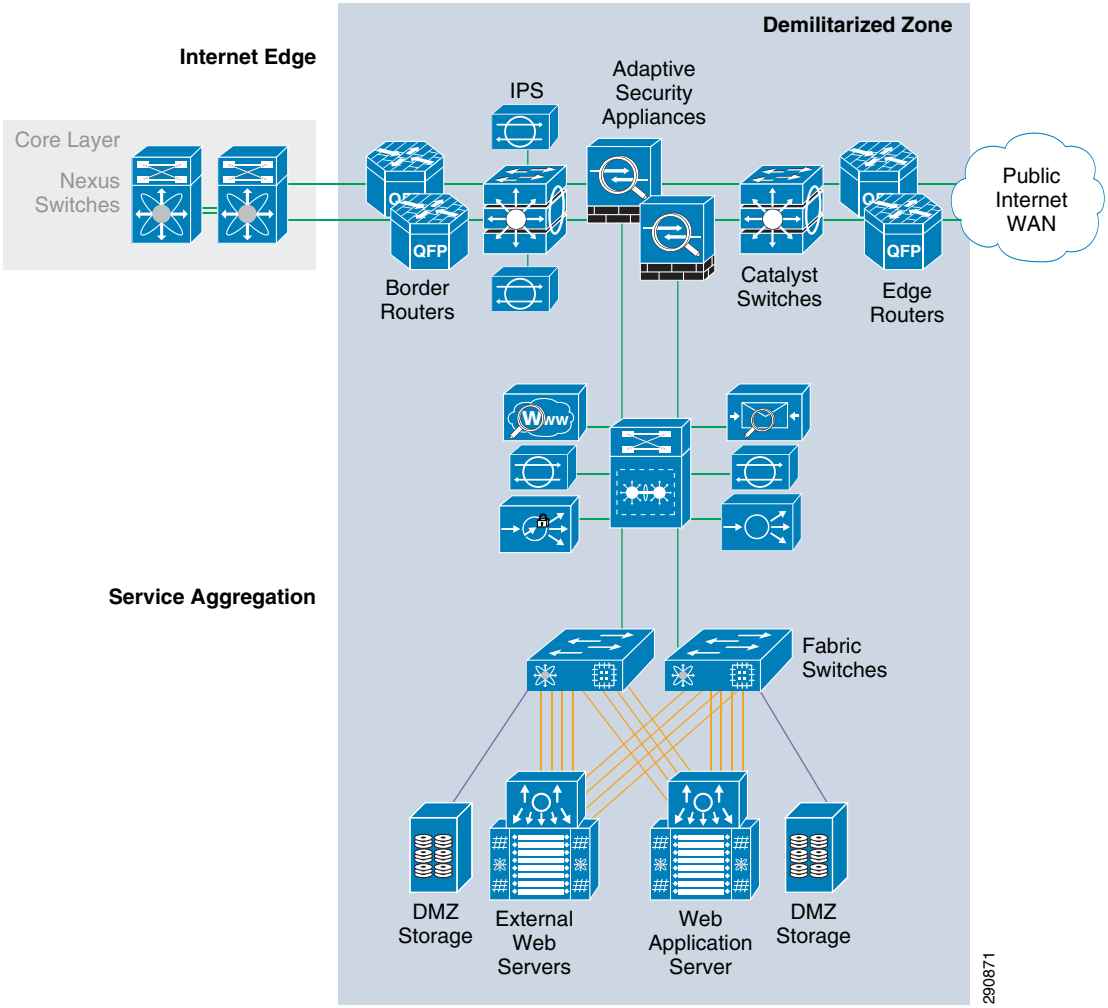
A subtle, yet potentially significant change to key management has been introduced with the PCI 2.0 standard. With past versions of the DSS, annual key rotations were required for encryption keys. DSS 2.0 now requires that keys are rotated at the end of their *cryptoperiod*, and references the NIST 800-57 Special Publication to determine what an appropriate cryptoperiod is. The NIST 800-57 Special Publication is a 324-page, three-part document. Organizations, and even QSAs, may not have the expertise to fully understand such a document that includes countless encryption scenarios, with cryptoperiods ranging from as short as a day to as long as three years.

In an ideal world, with all parties being expert cryptographers, this risk-based change to the standard would be very appropriate and most welcome. However, given the number of scenarios and criteria for determining an appropriate cryptoperiod, it could suggest that this change is too subjective and may become a point of contention between an organization and QSA assessor, as to what is an appropriate cryptoperiod; whereas the former, more prescriptive control, did not allow for flexibility in this area.

E-commerce/Internet Edge/Service Provider Edge/Partner Edge

The solution uses a collapsed Internet edge and extranet network to support Internet connectivity and business partner connectivity, as shown in Figure 3-14.

Figure 3-14 E-commerce/Internet Edge/Service Provider Edge



Design Considerations

The design does the following:

- Provides an enterprise connection to the Internet
- Secures the Internet edge design using Cisco firewall and intrusion detection systems
- Provides a dual-threaded design for network resiliency
- Provides a collapsed Internet edge and extranet network for a highly centralized and integrated edge network
- Provides remote VPN access to enterprise users/telecommuters

This design takes into account best practices from the *Data Center Networking: Internet Edge Design Architecture Design Guide* (http://www.cisco.com/go/designzone) and customizes these recommendations for the Internet edge and extranet networks of enterprises. The edges connect Internet services to the complete enterprise environment (that is, from headquarters to Internet service providers), and branch office connections that use a Cisco secure VPN to connect to headquarters. The collapsed design provides highly centralized and integrated edge networks, and transports the aggregated traffic through various service modules (Cisco ACE, Cisco ASASM, and Cisco IDSM2) within a pair of Cisco Catalyst 6500 Switch chassis. The Internet edge provides the following security functions:

- Secure configurations and management.
- IP anti-spoofing.
- Access control lists (ACLs) that provide explicitly permitted and/or denied IP traffic that may traverse between inside, outside, and DMZ.
- Stateful inspection provides the ability to establish and monitor session states of traffic permitted to flow across the Internet edge, and to deny traffic that fails to match the expected state of existing or allowed sessions.
- Intrusion detection using Cisco IDSM2 provides the ability to promiscuously monitor traffic across discrete points within the Internet edge, and to alarm and/or take action after detecting suspect behavior that may threaten the enterprise network.
- Applications servers that need to be directly accessed from the Internet are placed in a quasi-trusted secure area (DMZ) between the Internet and the internal enterprise network, which allows internal hosts and Internet hosts to communicate with servers in the DMZ.
- All public-facing web applications should be developed using the security best practices to prevent known attacks, and must be reviewed annually or after changes.

Enterprise Architecture and PCI Design Considerations



CHAPTER 4

Solution Implementation

Overview

Cisco customers have asked Cisco to provide insight into how Cisco products can be used to address PCI DSS 2.0 requirements. To fully accomplish this goal, Cisco hired an auditor and went through the same process as organizations. To audit Cisco products for the capability to address compliance, they had to be installed and configured within a representative design.

This chapter demonstrates how the Cisco PCI solution was installed and configured to address the specifications of PCI 2.0. Cisco partnered with RSA, HyTrust, EMC, VCE, and Verizon Business to create a comprehensive design that reflected the framework and architectural principles discussed in earlier chapters.

The Cisco PCI solution was validated in the Cisco Lab in San Jose, California. The branches, data center, WAN, and Internet edge network infrastructures were built using Cisco best practice design guides, as represented by the Cisco enterprise architecture (http://www.cisco.com/go/designzone). The individual components were installed and configured to adhere to PCI 2.0 specifications. Verizon Business then conducted an assessment of the design and advised on remediation for specific configurations of individual components. After the remediation was complete, Verizon Business provided a detailed reference architecture report (see Appendix C, "Verizon Business Reference Architecture Report—Cisco PCI Solution.")

Tip An ***architecture*** is a strategic structure for the consistent design, construction, and operation of systems to achieve a desired set of outcomes.

A ***design*** is a tactical implementation of an architectural strategy, using specific configurations of products to satisfy business requirements.

Chapter 3, "Solution Architecture," describes the enterprise architecture with regards to compliance. This chapter demonstrates a design or, in other words, a specific implementation of components to achieve these principles. Various designs can result from the solution architecture. The design that was implemented is not intended to represent the only way that Cisco and partner products can be installed to address PCI. It is intended to provide an example showing how and what was used to achieve the principles described in Chapter 3, "Solution Architecture."

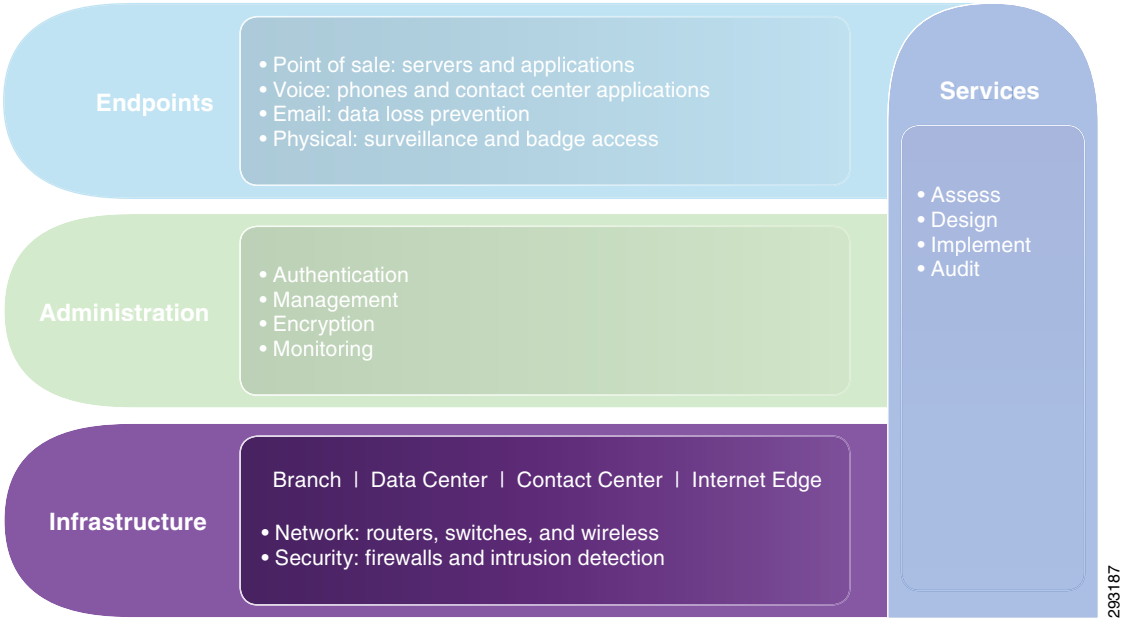
Although every company has specific considerations that vary from this implementation, these designs and the configurations of the components in Appendix E, "Detailed Full Running Configurations," provide an instructive example of what is needed to secure credit card data. Each component selected was audited for its capabilities, and that assessment is covered in the next chapter.

In each section, the reference architecture is shown with the corresponding design that was implemented and validated within the Cisco PCI laboratories. The full configurations of each individual component are available in Appendix E, "Detailed Full Running Configurations."

Infrastructure

The infrastructure layer of the solution framework addresses the components such as routers, switches, firewalls, and security components, as shown in Figure 4-1.

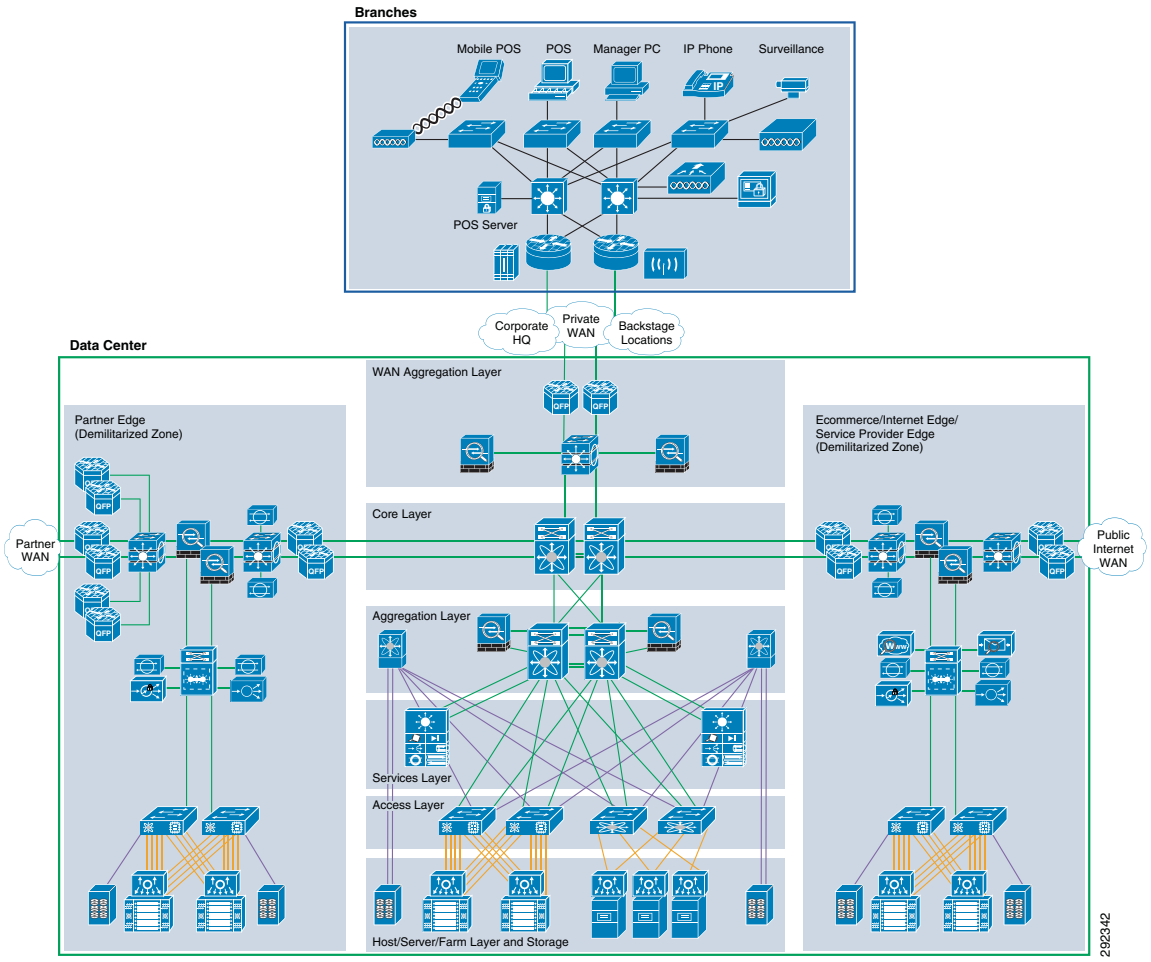
Figure 4-1 Infrastructure Layer of the Solution Framework



The following sections describe the designs that were implemented from the reference architecture.

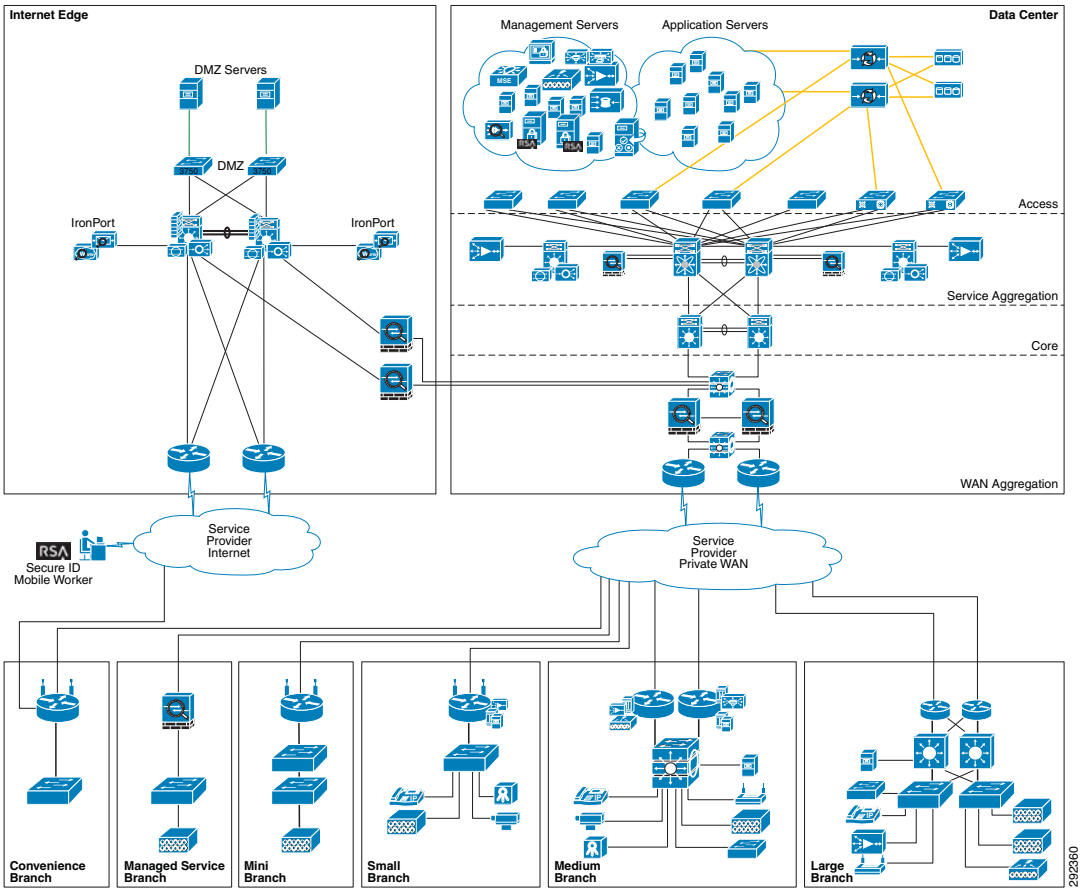
Figure 4-2 shows the enterprise-wide reference architecture.

Figure 4-2 Enterprise-Wide Reference Architecture



Referencing the enterprise-wide architecture shown in Figure 4-2, the design shown in Figure 4-3 was created in the Cisco Lab.

Figure 4-3 Cisco PCI Solution Lab Architecture



Note the following:

- Six branch designs were selected to represent Cisco and partner products.
- The data center consists of a single aggregation block based on the Data Center 3.0 architecture.
- The Internet edge is representative of both the e-commerce and partner edge for the purposes of validation.

The following sections describe this enterprise-wide design in more detail, and demonstrate what was implemented within the lab.

Branches

Multiple branch footprints were implemented that address a variety of business objectives. Each branch footprint section contains designs that were extracted from the reference architecture. Each design contains the following:

- Reference architecture
- Branch design
  - Logical topology
  - Addressing plan
  - Components selected

For component compliance functionality, see Chapter 5, "Component Assessment.". For full device configurations, see Appendix E, "Detailed Full Running Configurations."

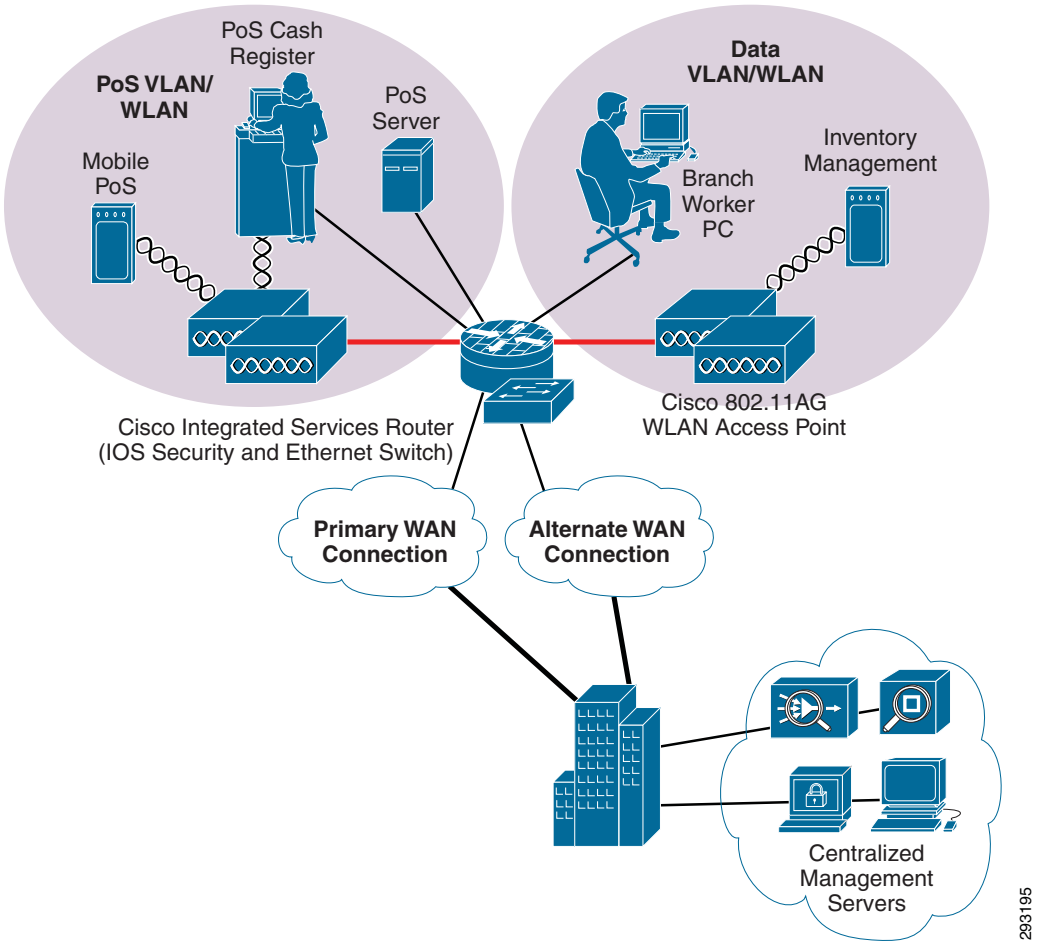
Note Each of these branch designs includes a variety of components that can be interchangeably used between them, depending on business requirements. For validation purposes, it was not necessary to implement all possible components in each design.

Small Branch Architecture

The small branch network scenario, shown in Figure 4-4, meets the following design requirements:

- Branch size averages between 2000–6000 square feet
- Fewer than 25 devices requiring network connectivity
- Single router with firewall/IPS, integrated Ethernet switch, compact switch, and power-over-Ethernet (PoE)
- Preference for integrated services within fewer network components because of physical space requirements
- Wireless connectivity

Figure 4-4 Small Branch Architecture



The small branch reference architecture is a powerful platform for running an enterprise that requires simplicity and a compact form factor. This combination appeals to many formats that can include the following:

- Small branch—Specialty shops, discount businesses
- Mini branches—Fuel stations, mall outlet
- Convenience branches—Pop-up stores, health centers, mall kiosks
- Managed service provider branch—WAN access controlled by service provider

This network architecture is widely used and consolidates many services into fewer infrastructure components. The small branch also supports a variety of business application models because an integrated Ethernet switch supports high-speed LAN services. In addition, an integrated content engine supports centralized application optimization requirements such as Web Cache Communications Protocol (WCCP)-based caching, pre-positioning of data, local media streaming, and other application velocity services.

Advantages include the following:

- Lower cost per branch
- Fewer parts to spare
- Fewer software images to maintain
- Lower equipment maintenance costs

Limitations include the following:

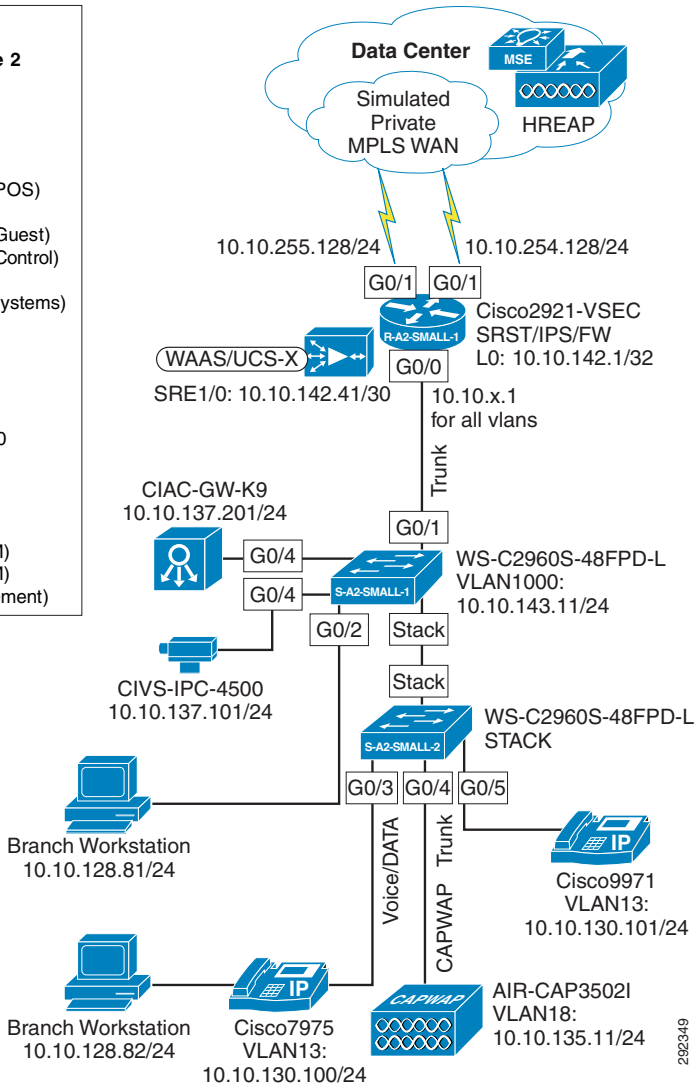
- Decreased levels of network resilience
- Greater potential downtime because of single points of failure

Small Branch—Small Design

Figure 4-5 shows the small branch network design.

Figure 4-5 Small Branch Network Design

Small Branch IP Addressing	
10.10.128.0 255.255.240.0	**Small Branch Aisle 2**
10.10.128.0 /24	VLAN11 (POS)
10.10.129.0 /24	VLAN12 (Data)
10.10.130.0 /24	VLAN13 (Voice)
10.10.131.0 /24	VLAN14 (Wireless)
10.10.132.0 /24	VLAN15 (Wireless POS)
10.10.133.0 /24	VLAN16 (Partner)
10.10.134.0 /24	VLAN17 (Wireless Guest)
10.10.135.0 /24	VLAN18 (Wireless Control)
10.10.136.0 /24	VLAN19 (WAE)
10.10.137.0 /24	VLAN20 (Security Systems)
10.10.138.0 /24	(Future)
10.10.139.0 /24	(Future)
10.10.140.0 /24	(Future)
10.10.141.0 /24	(Future)
10.10.142.0 /24	Other- (Misc)
10.10.142.1 /32	R-A2-Small-1 Loop 0
10.10.142.16 /30	(Future)
10.10.142.20 /30	(Future)
10.10.142.24 /30	(Future)
10.10.142.28 /30	(Future)
10.10.142.32 /29	VLAN 110 (SRE-SM)
10.10.142.40 /30	VLAN 111 (SRE-SM)
10.10.143.0 /24	VLAN1000 (Management)



Components Selected

- Cisco 2921 Integrated Services Router (ISR)
- Cisco Catalyst 2960S 48-port PoE Switch
- Cisco Aironet 3502i Access Points
- Cisco Video Surveillance 4500 Series IP Cameras
- Cisco Physical Access Gateway

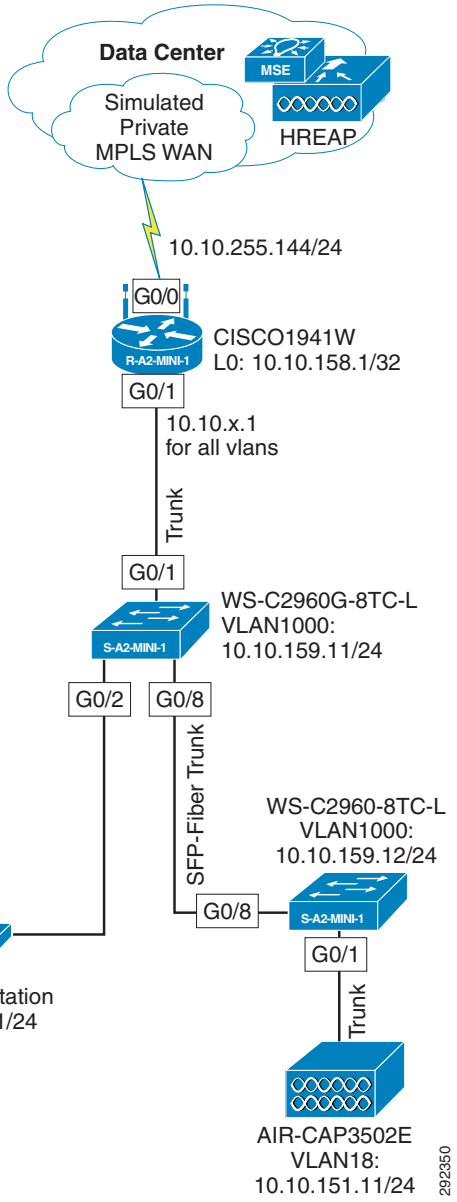
Small Branch—Mini Design

The mini branch represents an alternate design for the small branch architecture, using different components.

Figure 4-6 shows the mini branch network design.

Figure 4-6 Mini Branch Network Design

Mini Branch IP Addressing	
10.10.144.0 255.255.240.0	**Mini Branch Aisle 2**
10.10.144.0 /24	VLAN11 (POS)
10.10.145.0 /24	VLAN12 (Data)
10.10.146.0 /24	VLAN13 (Voice)
10.10.147.0 /24	VLAN14 (Wireless)
10.10.148.0 /24	VLAN15 (Wireless POS)
10.10.149.0 /24	VLAN16 (Partner)
10.10.150.0 /24	VLAN17 (Wireless Guest)
10.10.151.0 /24	VLAN18 (Wireless Control)
10.10.152.0 /24	VLAN19 (WAE)
10.10.153.0 /24	(Future)
10.10.154.0 /24	(Future)
10.10.155.0 /24	(Future)
10.10.156.0 /24	(Future)
10.10.157.0 /24	(Future)
10.10.158.0 /24	Other- (Misc)
10.10.158.1 /32	R-A2-Mini-1 Loop 0
10.10.158.16 /30	(Future)
10.10.158.20 /30	(Future)
10.10.158.24 /30	(Future)
10.10.158.28 /30	(Future)
10.10.158.32 /29	VLAN 110 (Wireless NM)
10.10.158.40 /30	VLAN 111 (WAE Management
10.10.159.0 /24	VLAN1000 (Management)



Components Selected

- Cisco 1941 Integrated Services Router (ISR)
- Cisco Catalyst 2960 Switch
- Cisco Aironet 3502e Access Point

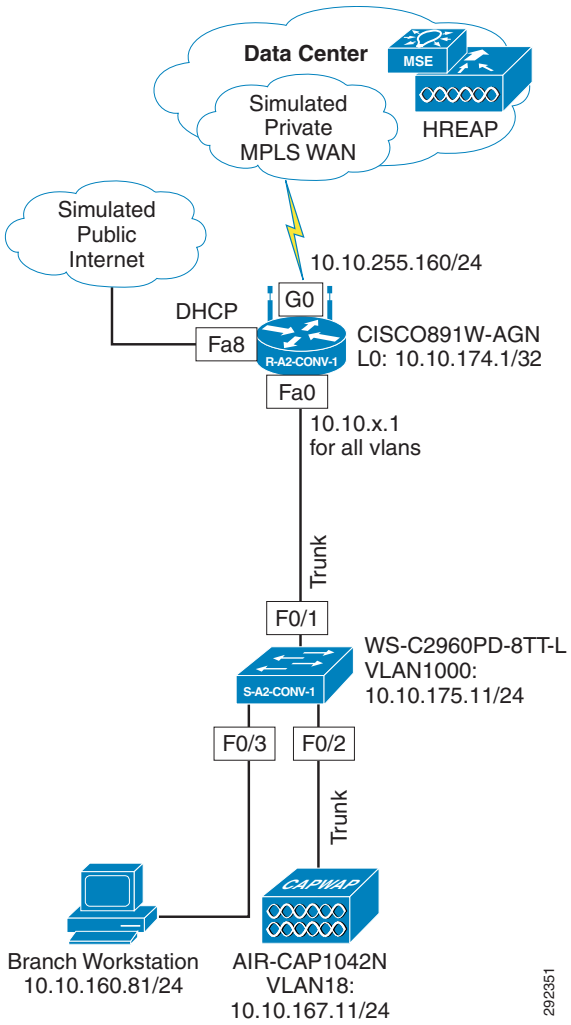
Small Branch—Convenience Design

The convenience branch represents an alternate design for the small branch architecture. Figure 4-7 shows the convenience branch network design.

Figure 4-7 Convenience Branch Network Design

Convenience Branch IP Addressing

10.10.160.0 255.255.240.0	Convenience Branch Aisle 2
10.10.160.0 /24	VLAN11 (POS)
10.10.161.0 /24	VLAN12 (Data)
10.10.162.0 /24	VLAN13 (Voice)
10.10.163.0 /24	VLAN14 (Wireless)
10.10.164.0 /24	VLAN15 (Wireless POS)
10.10.165.0 /24	VLAN16 (Partner)
10.10.166.0 /24	VLAN17 (Wireless Guest)
10.10.167.0 /24	VLAN18 (Wireless Control)
10.10.168.0 /24	VLAN19 (WAE)
10.10.169.0 /24	(Future)
10.10.170.0 /24	(Future)
10.10.171.0 /24	(Future)
10.10.172.0 /24	(Future)
10.10.173.0 /24	(Future)
10.10.174.0 /24	Other- (Misc)
10.10.174.1 /32	R-A2-Conv-1 Loop 0
10.10.174.16 /30	(Future)
10.10.174.20 /30	(Future)
10.10.174.24 /30	(Future)
10.10.174.28 /30	(Future)
10.10.174.32 /29	(Future)
10.10.174.40 /30	(Future)
10.10.175.0 /24	VLAN1000 (Management)



Components Selected

- Cisco 891 Series Integrated Services Router (ISR)
- Cisco Catalyst 2960 Series Switch
- Cisco Aironet 1042N Access Point

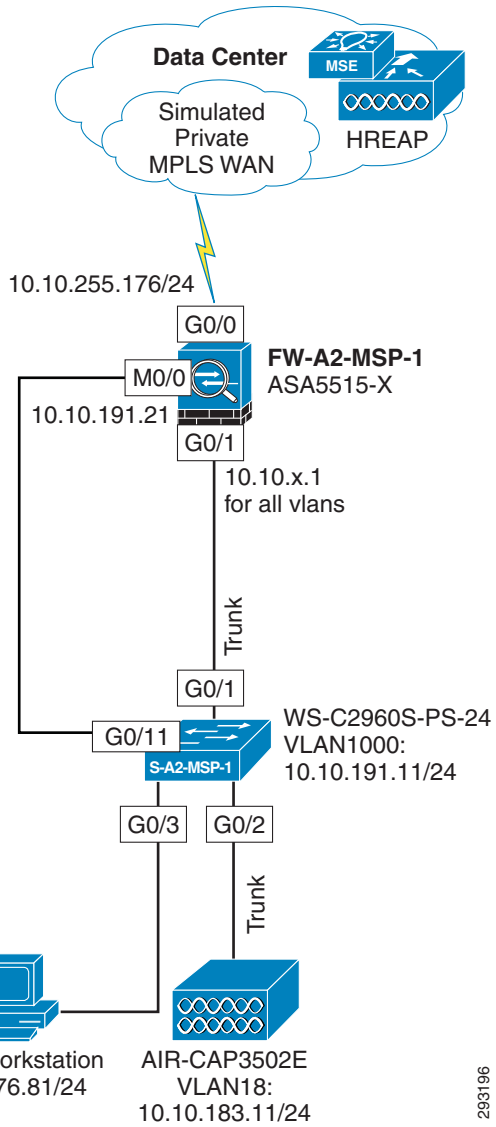
Small Branch—Managed Service Provider Design

The managed service provider branch represents an alternate design for the small branch architecture. Figure 4-8 shows the managed service provider network design.

Figure 4-8 Managed Service Provider Branch Network Design

Managed Service Provider Branch IP Addressing

10.10.176.0 255.255.240.0	MSP Branch Aisle 2
10.10.176.0 /24	VLAN11 (POS)
10.10.177.0 /24	VLAN12 (Data)
10.10.178.0 /24	VLAN13 (Voice)
10.10.179.0 /24	VLAN14 (Wireless)
10.10.180.0 /24	VLAN15 (Wireless POS)
10.10.181.0 /24	VLAN16 (Partner)
10.10.182.0 /24	VLAN17 (Wireless Guest)
10.10.183.0 /24	VLAN18 (Wireless Control)
10.10.184.0 /24	VLAN19 (WAE)
10.10.185.0 /24	(Future)
10.10.186.0 /24	(Future)
10.10.187.0 /24	(Future)
10.10.188.0 /24	(Future)
10.10.189.0 /24	(Future)
10.10.190.0 /24	Other- (Misc)
10.10.190.1 /32	R-A2-MSP-1 Loop 0
10.10.190.16 /30	SP to FW link
10.10.190.20 /30	(Future)
10.10.190.24 /30	(Future)
10.10.190.28 /30	(Future)
10.10.190.32 /29	(Future)
10.10.190.40 /30	(Future)
10.10.191.0 /24	VLAN1000 (Management)



Components Selected

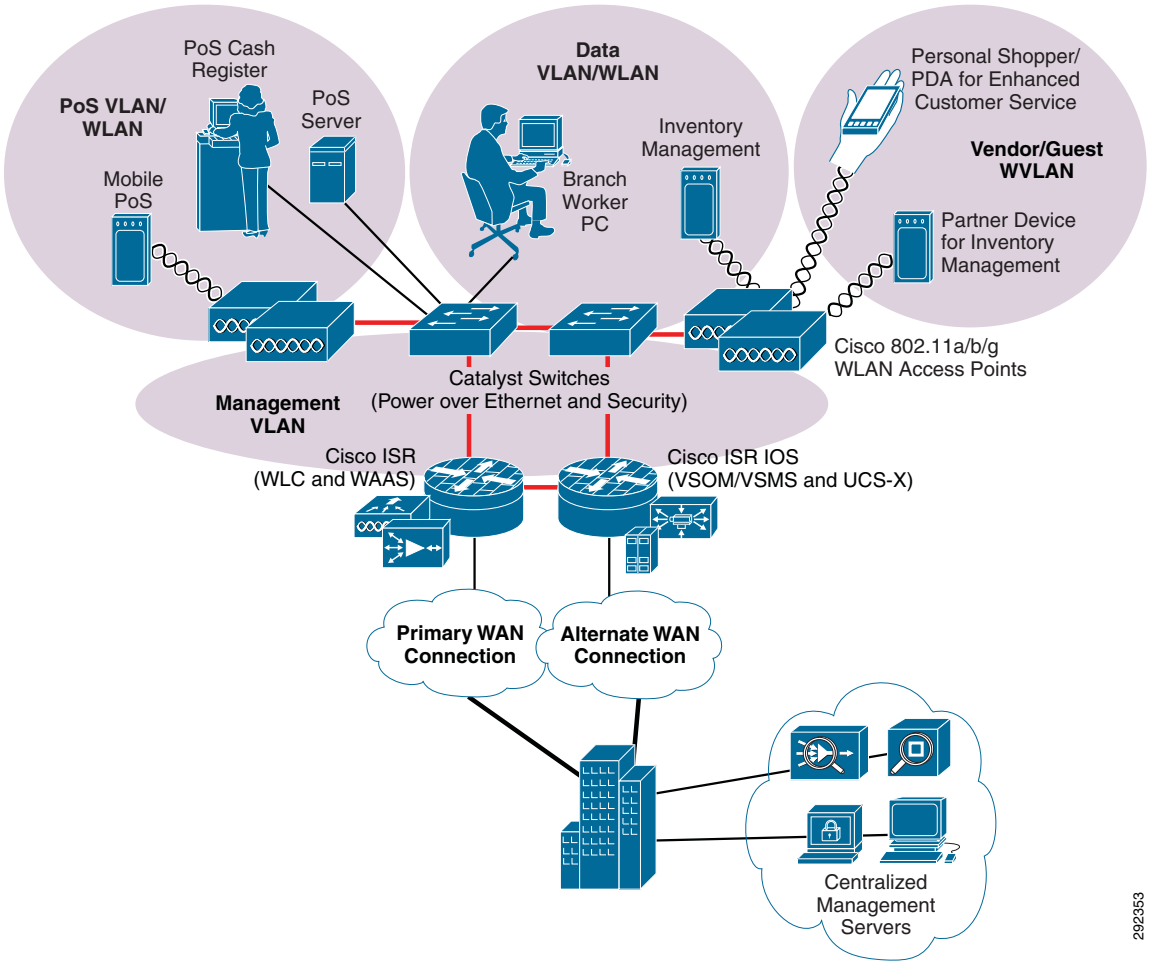
- Cisco ASA 5510 Firewall with SSM-10
- Cisco Catalyst 3560E Switch
- Cisco Aironet 3502e Access Points

Medium Branch Architecture

The medium branch network scenario, shown in Figure 4-9, meets the following design requirements:

- Branch size averages between 6,000–18,000 square feet
- The physical size of the branch is smaller than a large branch, so a distribution layer of network switches is not required
- Number of devices connecting to the network averages 25–100 devices
- Redundant LAN and WAN infrastructures with firewall/IPS
- Wireless connectivity

Figure 4-9 Medium Branch Architecture



The medium branch reference architecture is designed for enterprise businesses that require network resilience and increased levels of application availability over the small branch architecture and its single-threaded, simple approach. As more mission-critical applications and services converge onto the IP infrastructure, network uptime and application availability are more important. The dual-router and dual-LAN switch design of the medium branch supports these requirements. Each of the Cisco ISR routers can run Cisco IOS Software security services and other branch communication services

simultaneously. Each of the Cisco ISR routers is connected to a dedicated WAN connection. Hot Standby Routing Protocol (HSRP) is used to ensure network resilience in the event that the network connection fails.

The access layer of the network offers enhanced levels of flexibility and more access ports compared to the small branch. Up to 12 wireless access points can be installed in the branch, supported by the Cisco Wireless Control System (WCS) controller as tested and without adding more controllers. The distributed Cisco Catalyst switches can support a combination of larger physical buildings or a larger number of endpoints than the small branch.

Advantages include the following:

- More adaptive access layer with support for a greater number of endpoints and more diverse building requirements (multiple floors, sub-areas, and so on)
- Improved network resilience through parallel device design
- Improved network and application availability through parallel paths

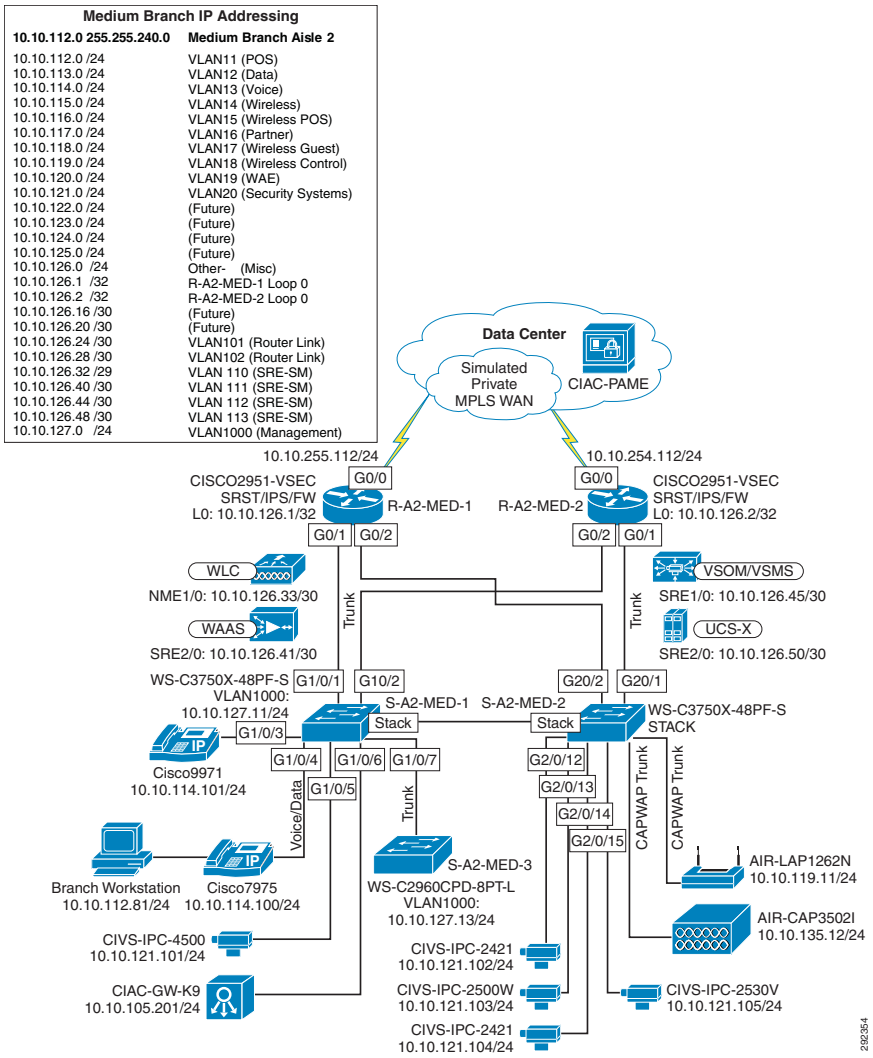
Limitations include the following:

- No distribution layer between core layer (the ISR) and the access layer switches
- Single WCS Controller decreases in-branch resilience of the wireless network; the recommendation is to have branch APs fallback to the central WCS controller if the local WCS controller fails, or to install dual-local WCS controllers.

Medium Branch—Design

Figure 4-10 shows the medium branch network design.

Figure 4-10 Medium Branch Network Design



Components Selected

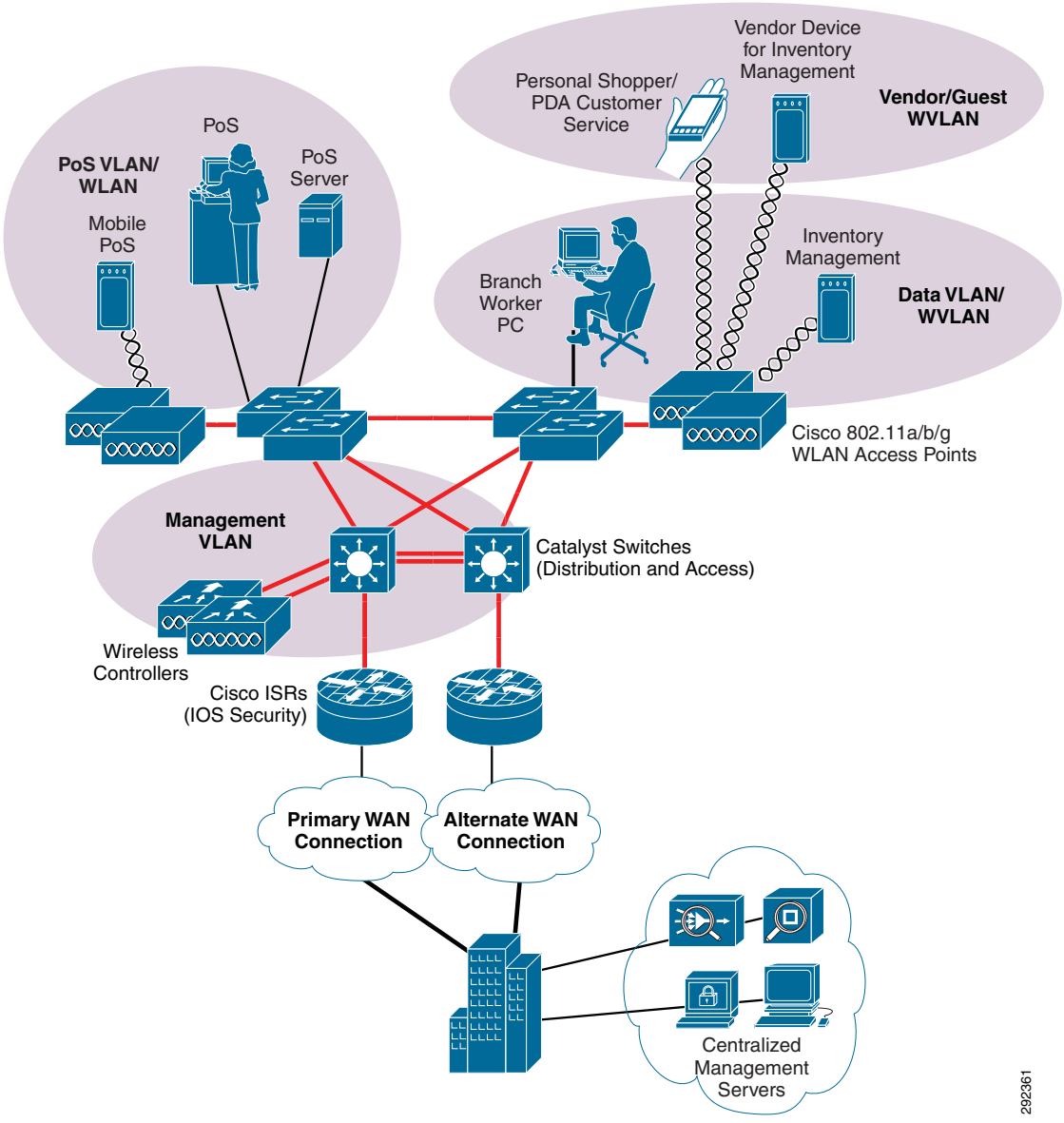
- Cisco 2951 Integrated Services Router (ISR)
- Cisco Catalyst 3750X 48-port PoE Switch
- Cisco Catalyst 2960 Compact Switch
- Cisco Aironet 3502e and 1262N Access Points
- Cisco Video Surveillance 2421 IP Dome Camera
- Cisco Video Surveillance 2500 Series IP Camera
- Cisco Operations Manager v4.1
- Cisco Physical Access Gateway

Large Branch Architecture

The large branch network scenario, shown in Figure 4-11, meets the following design requirements:

- Branch size averages between 15,000–150,000 square feet
- More than 100 devices per branch requiring network connectivity
- Multiple routers with firewall/IPS for primary and backup network requirements
- Preference for a combination of network services distributed within the branch to meet resilience and application availability requirements
- Tiered network architecture within the branch; distribution layer switches are employed between the central network services core and the access layer connecting to the network endpoints (POS, wireless APs, servers)

Figure 4-11 Large Branch Architecture



The large branch reference architecture takes some of the elements of Cisco campus network architecture recommendations and adapts them to a large branch environment. Network traffic can be better segmented (logically and physically) to meet business requirements. The distribution layer of the large branch architecture can greatly improve LAN performance while offering enhanced physical media connections (that is, fiber and copper for connection to remote access layer switches and wireless access points). A larger number of endpoints can be added to the network to meet business requirements. This type of architecture is widely used by large format organizations globally. Dual routers and distribution layer media flexibility greatly improve network serviceability because the network is highly available and scales to support the large branch requirements. Routine maintenance and upgrades can be scheduled and performed more frequently or during normal business hours because of parallel path design.

Advantages include the following:

- Highest network resilience based on highly available design
- Port density and fiber density for large locations
- Increase segmentation of traffic
- Scalable to accommodate shifting requirements in large branches

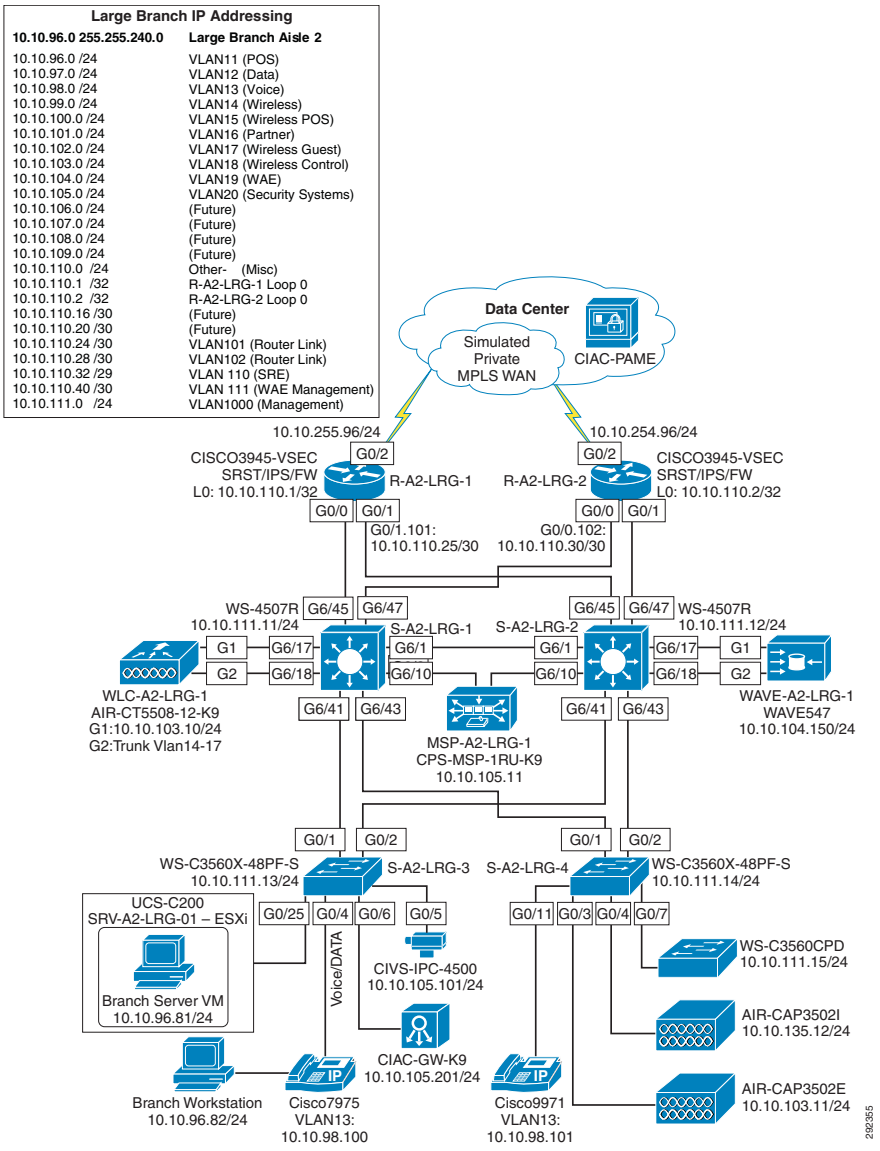
Limitations include the following:

- Higher cost because of network resilience based on highly available design
- These branch network designs are capable of helping an organization achieve PCI compliance, and also serve as the scalable platform for new services and applications

Large Branch Design

Figure 4-12 shows the large branch network design.

Figure 4-12 Large Branch Network Design



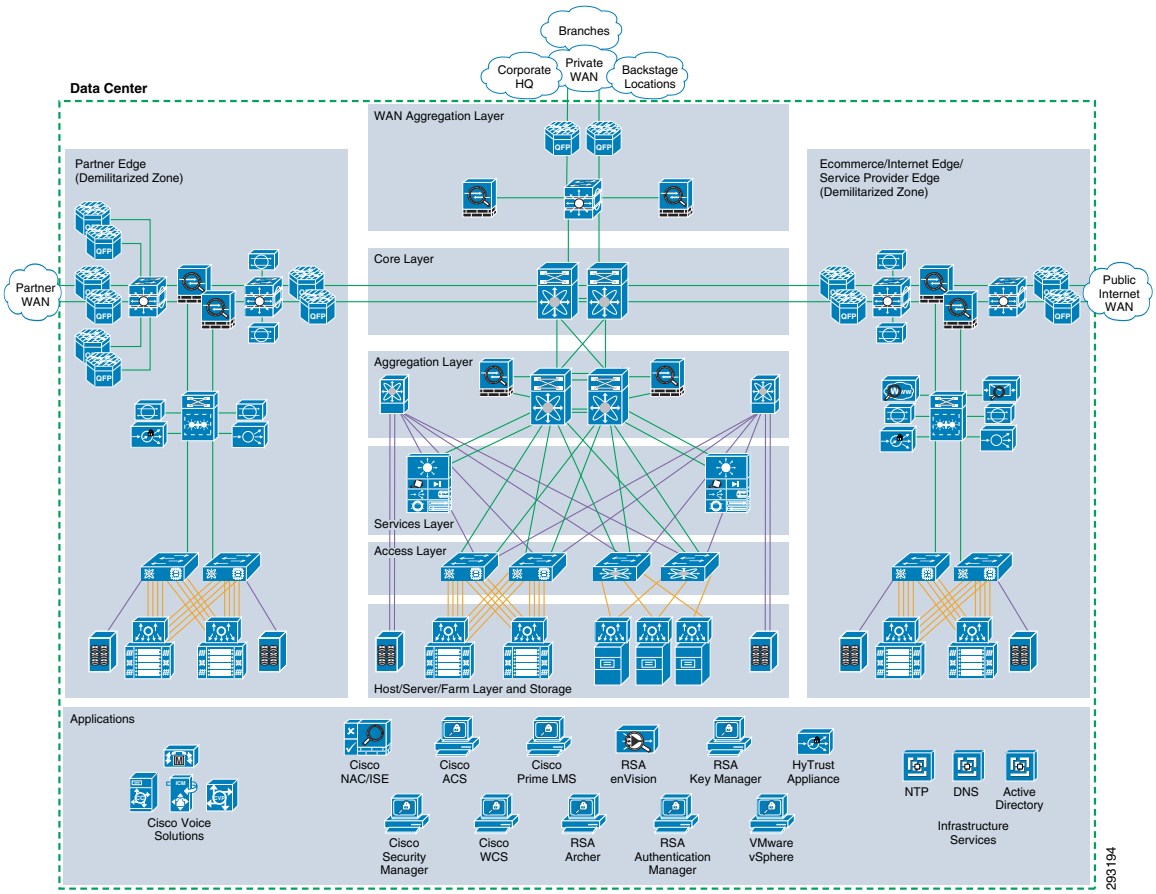
Components Selected

- Cisco 3945 Integrated Services Router (ISR)
- Cisco Catalyst 3560X and 4500 switches
- Cisco Aironet 3502e and 3502i Access Points
- Cisco 5508 Wireless Controller
- Cisco 4500 Video Surveillance Camera
- Cisco Physical Access Gateway

Data Center

The data center is where centralized data processing, data storage, and data communications take place (see Figure 4-13). The data center is also the place where management systems are deployed. The data center provides centralized control from an administrative perspective because it is typically where the tools that are used to monitor and enforce compliance are deployed.

Figure 4-13 Data Center Architecture



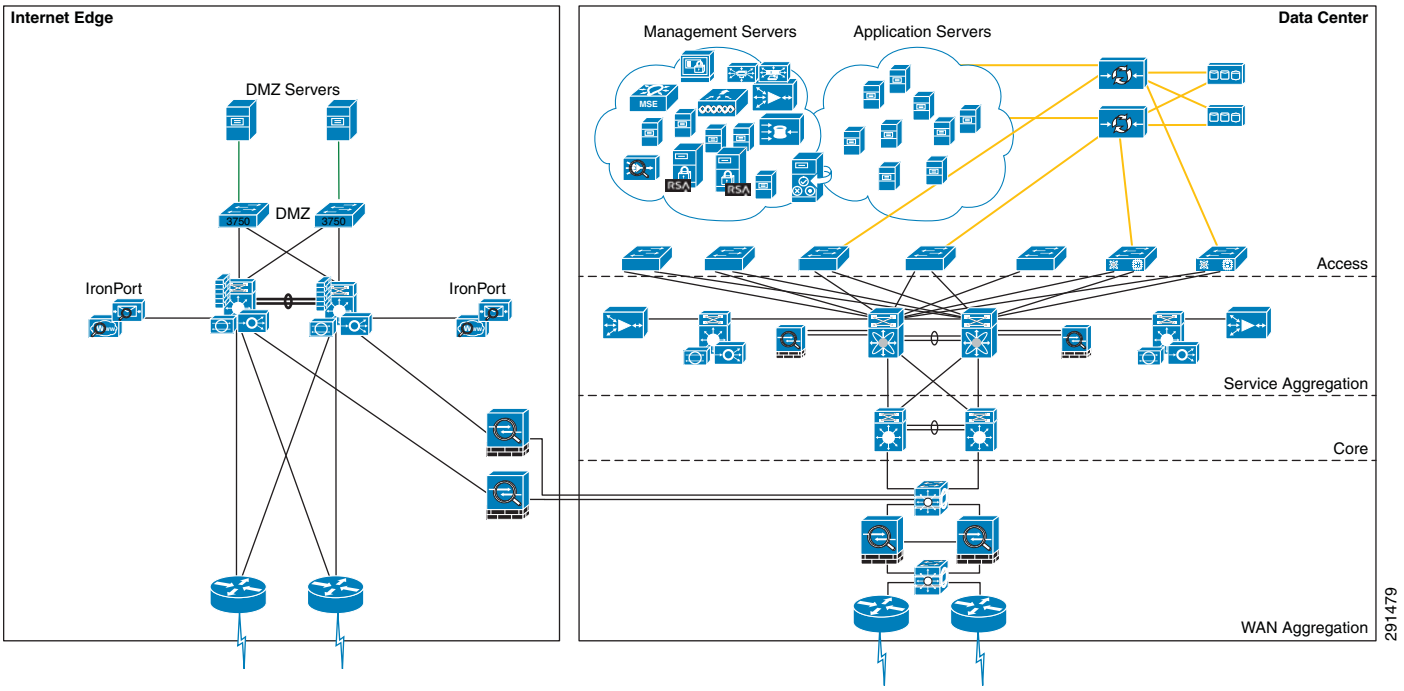
Design considerations are as follows:

- Centralized solution management supports all aspects of network, security, and systems management; and supports remote access from anywhere on the network.
- Standardized equipment and software images, deployed in a modular, layered approach, simplify configuration management and increase the systems availability.
- The highly available data center design permits highly resilient access from branches to core data and storage services.
- WAN aggregation alternatives allow flexible selection of service provider network offerings.
- The service aggregation design allows for a modular approach to adding new access layers and managing shared network services (for example, firewall, IPS, application networking, wireless management)

- Firewall, IPS, and application networking services are available at the service and aggregation layers of the data center.
- Scalability to accommodate shifting requirements in data center compute and storage requirements.
- WAN access speeds are typically the limiting factor between the branch network systems and the WAN aggregation layer.
- It is typical for organizations to over-subscribe the WAN circuits between the branches and the WAN edge aggregation router. Over-subscription can cause inconsistent results and packet loss of payment card information in the event that more traffic enters the WAN circuit simultaneously.
- Backup network connections from branch networks to the data center are recommended when payment card information is transported via the WAN.

Figure 4-14 shows the data center design.

Figure 4-14 Data Center Design



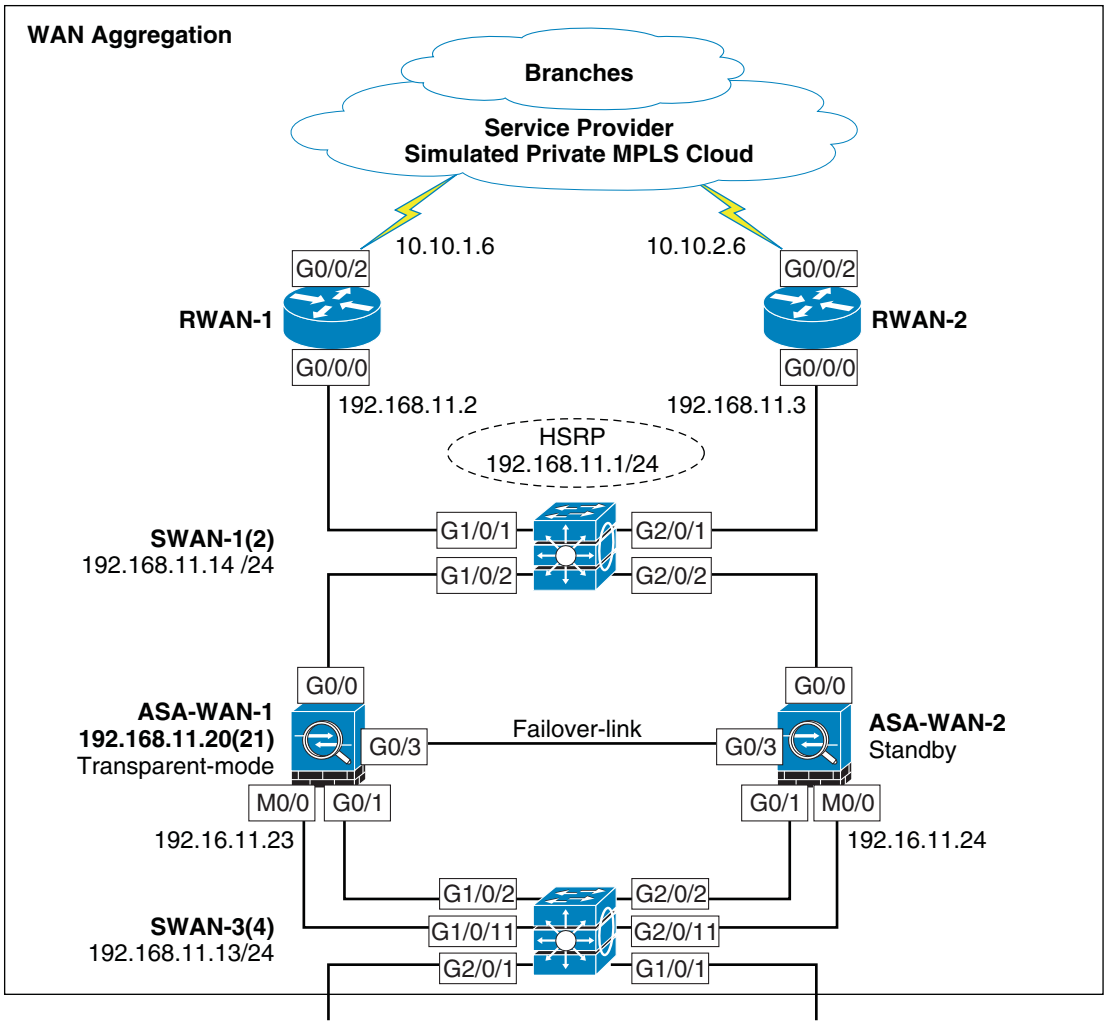
Data centers can house many types of functions and the term itself can encompass narrow and broad aspects. For the purposes of this guide, data centers include the following functions:

- WAN aggregation layer—Aggregates the branch and backstage WAN connections to the core
- Core layer—Highly available, high-speed area that is the central point of connectivity to all data center areas
- Aggregation block—Aggregates the services of one area and connects that area to the core, including Vblock1 design
- Internet edge—Secure connectivity to the Internet

WAN Aggregation Layer Design

Figure 4-15 shows the WAN aggregation layer design.

Figure 4-15 WAN Aggregation Layer Design



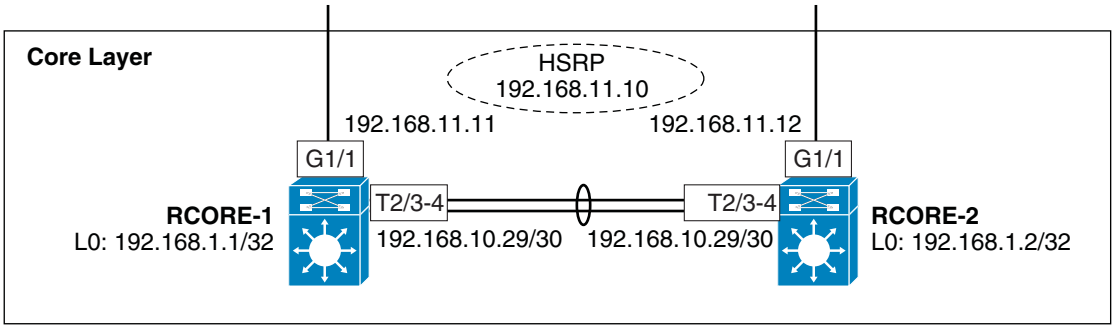
Components Selected

- Cisco ASR 1002-Fixed Router
- Cisco ASA 5540 Adaptive Security Appliance
- Cisco Catalyst 3750X Switch

Core Layer Design

Figure 4-16 shows the core layer design.

Figure 4-16 Core Layer Design



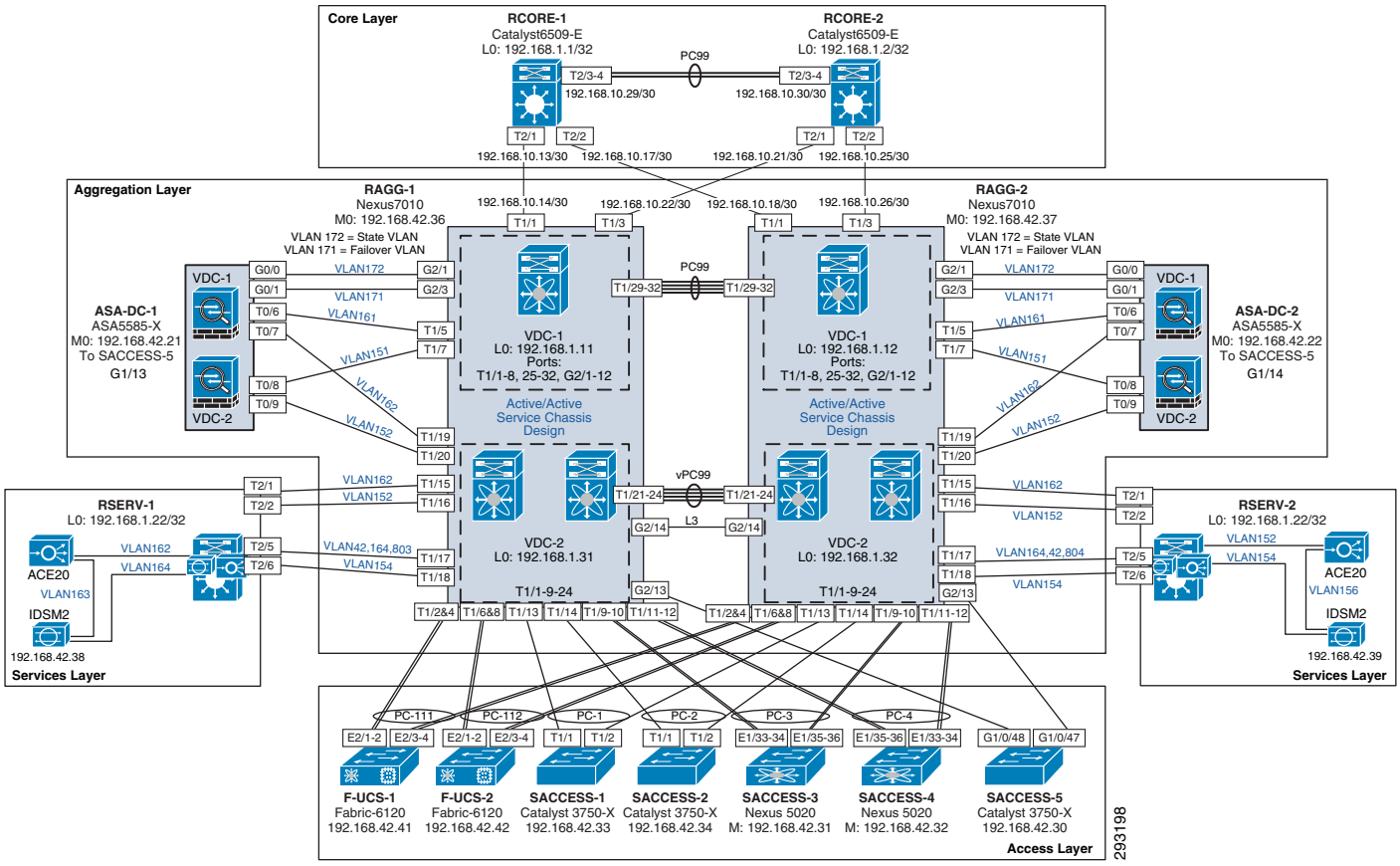
Components Selected

- Cisco Catalyst 6500-E Switch

Aggregation Block Design

Figure 4-17 shows the aggregation block design.

Figure 4-17 Aggregation Block Design



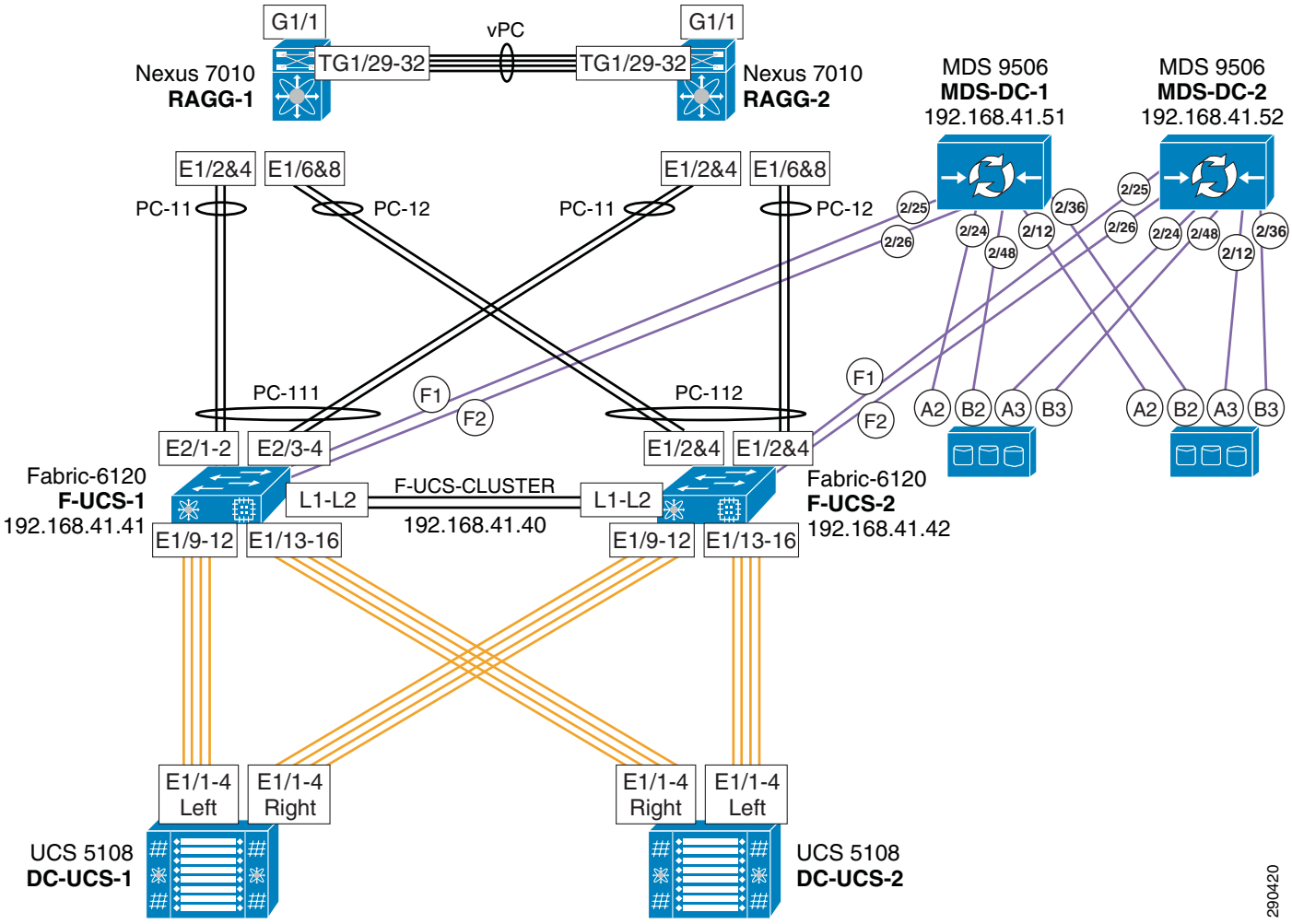
Components Selected

- Cisco ASA 5585-X Adaptive Security Appliance
- Cisco Nexus 7010 Switch
- Cisco Catalyst 6500-E Switch
  - Cisco ACE 20
  - Cisco IDSM-2
- Cisco Nexus 5020 Switch
- Cisco Catalyst 4948 Switch

Vblock Design

Figure 4-18 shows the Vblock design.

Figure 4-18 Vblock Design



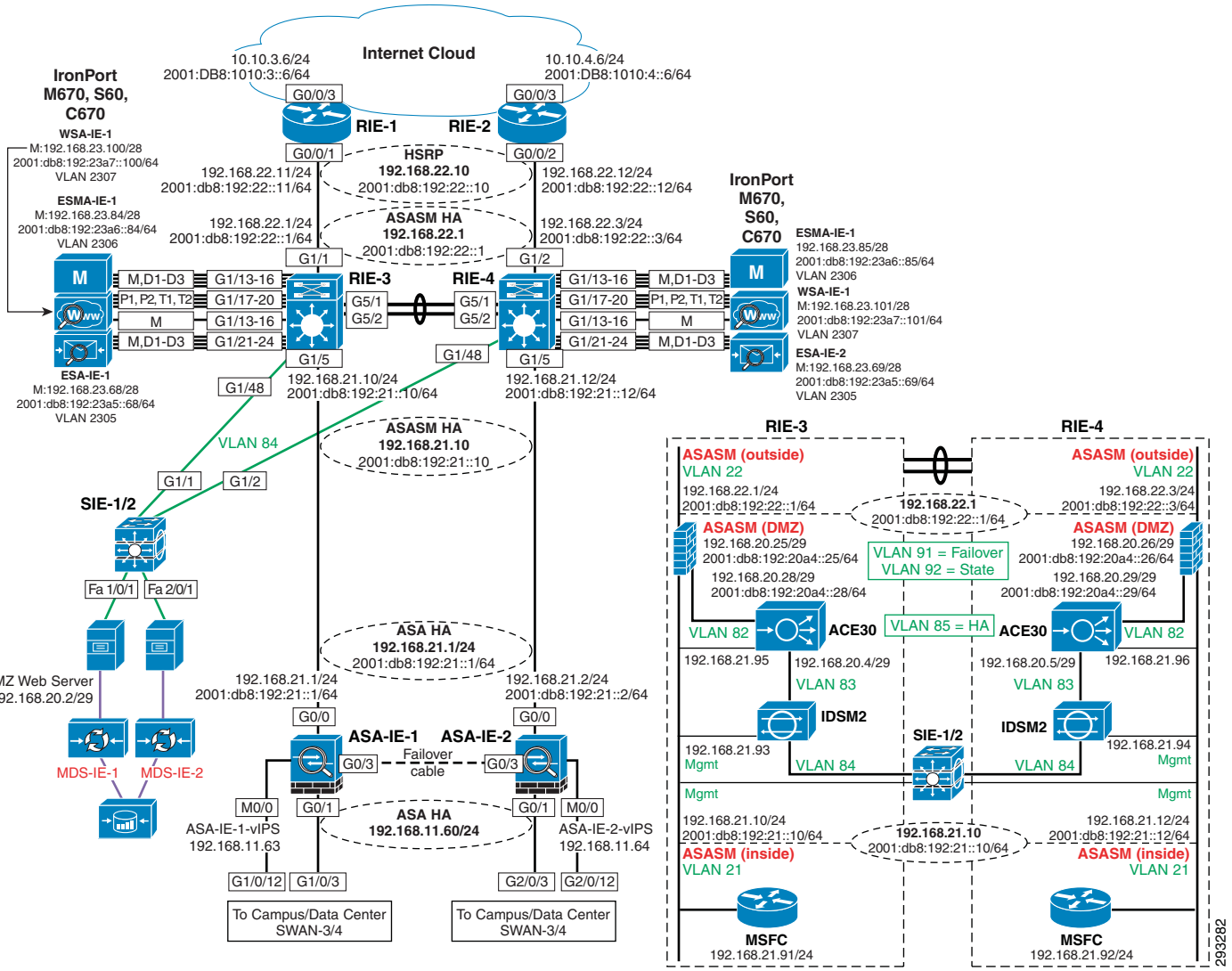
Components Selected

- Cisco UCS 5108 Blade Server Chassis
  - Cisco UCS B200 Blade Server
- Cisco UCS 6120 Fabric Interconnect
- Cisco MDS 9506 Multilayer Director
- EMC CLARiion CX4 Model 240

Internet Edge Design

Figure 4-19 shows the Internet edge network design.

Figure 4-19 Internet Edge Network Design



Components Selected

- Cisco 7200 Series Router
- Cisco Catalyst 6500-E Switch
  - Cisco ACE 20
  - Cisco IDSM-2
- Cisco Catalyst 3750X Switch
- Cisco MDS 9204i Switch
- Cisco IronPort C670

Addressing and Routing Disclosure

PCI requirement 1.3.8 states that merchants must not disclose private addressing and routing information. An enterprise contains two segments:

- Public—Where Internet services are hosted
- Private—Where internal systems reside that are not directly accessible from outside the company

Both may be deployed internally within an enterprise data center or other PIN. The private information must be protected and not propagated out to untrusted parties.

In 2013, it is common for enterprises to deploy an IPv6 Internet presence by using the Server Load Balancing (SLB) to do protocol family translation; that is, when the SLB receives an IPv6 inbound connection from the Internet, the SLB translates this connection on the fly into an IPv4 connection to the real servers.

In this solution, PCI 1.3.8 was met because all the security pieces for IPv4 are also used for IPv6 connections. Moreover, the servers where the information resides have no IPv6 addresses and cannot be reached over IPv6. The attack surface of the servers is strictly the IPv4 attack surface.

Note For more information on the Cisco ACE Application Control Engine Module, see the following URL: http://www.cisco.com/en/US/products/ps6906/index.html.

A best practice when implementing IPv6 is a phased approach. Figure 4-20 illustrates the scenario described above as the first phase of an IPv6 deployment.

Figure 4-20 IPv6 Phased Approach

PHASE 1

Initial deployments of IPv6 require that only the Internet edge routing, firewalling and load balancing systems need to support IPv6. By performing IPv6 to IPv4 NAT in the load balancer, downstream systems such as IDS, reverse web proxies and Web servers only need to support the IPv4 protocol. This can save a lot of time and investment making your services available to the growing IPv6 community of customers and merchants.

PHASE 2

Complete deployments of IPv6 require updating of all systems that will need to support IPv6.

If that is not possible because of legacy systems and applications, you can advance your enterprise addressing in phases by performing IPv4 to IPv6 NAT in the Web Proxy.

This step allows all Enterprise clients to be able to access new services that will only available via IPv6.

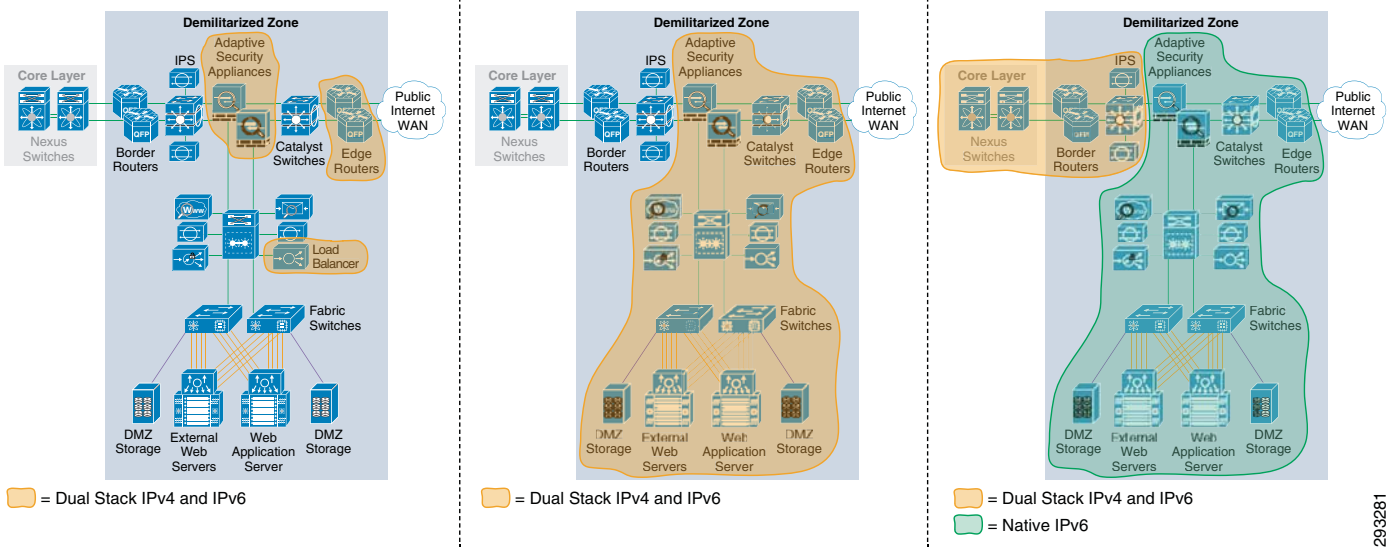
This can save time and investment providing access to cloud services before transitioning the enterprise to IPv6.

PHASE 3

Simplification of infrastructure can be achieved when a majority of Internet services and traffic are available via IPv6.

Removing IPv4 protocol in the enterprise wherever possible will simplify management, configuration and security of the infrastructure.

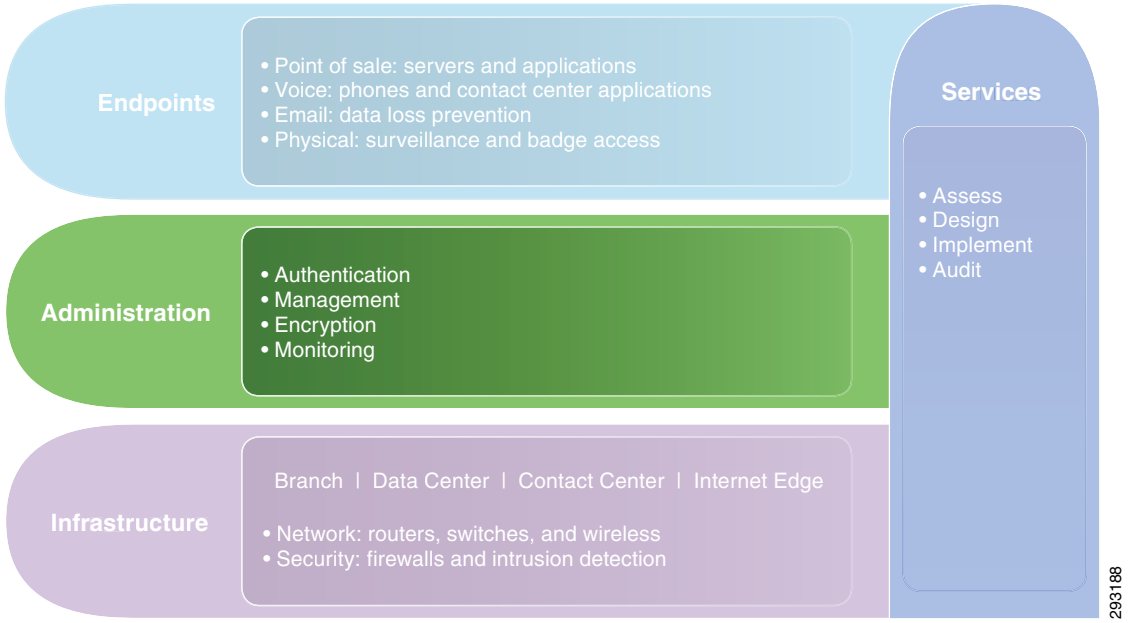
Internet Edge firewalls will still need to be configured to support IPv4 to IPv6 NAT for legacy systems until they can be transitioned or retired.



Administration

The administration layer of the solution framework addresses the components such as authentication, encryption, management, and monitoring, as shown in Figure 4-21.

Figure 4-21 Administration Layer of the Solution Framework



Authentication

Components Selected

- Cisco Secure Access Control Server (ACS)
- Cisco Identity Services Engine (ISE)
- RSA Authentication Manager
- Windows Active Directory

Encryption

Components Selected

- Cisco Security Manager
- Cisco Key Manager
- RSA Data Protection Manager

Management

Components Selected

- Cisco Prime LAN Management Solution (LMS)

- Cisco Security Manager
- Cisco Wireless Control Server Manager
- EMC Unified Infrastructure Manager
- VMware vSphere vCenter
- Cisco Video Surveillance Manager
- Cisco Physical Access Manager
- RSA Archer

Monitoring

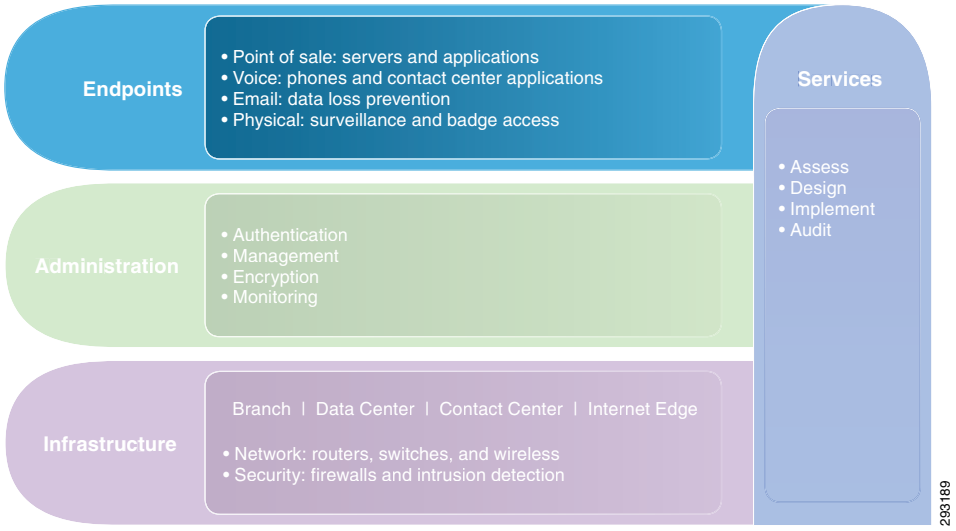
Components Selected

- RSA enVision
- HyTrust

Endpoints

The endpoints layer of the solution framework addresses the components such as voice, e-mail, and physical security, as shown in Figure 4-22.

Figure 4-22 Endpoints Layer of the PCI Solution Framework



Voice

Components Selected

- Cisco Unified Communications Manager

- Cisco IP Phones (9971, 7975)
- Cisco Survivable Remote Site Telephony (SRST)

E-mail

Components Selected

- Cisco IronPort Email Security Appliance with Data Loss Prevention
- Microsoft Exchange Server 2008

Physical

Components Selected

- Cisco Physical Access Gateway
- Cisco Video Surveillance Cameras (2421, 2500, 4500)

Note For a complete Bill of Materials, see Appendix A, "Bill Of Material." For assessment of components selected for PCI compliance, see Chapter 5, "Component Assessment." For complete running configurations of components, see Appendix E, "Detailed Full Running Configurations."

PCI Solution Result Summary

Cisco Compliance Solution Components

This solution combines components to create an end-to-end solution conforming to the requirements of the PCI 2.0 guidelines. The result is a set of branch, data center, and Internet edge architectures and designs that simplify the process of achieving and maintaining compliance.

Endpoints	Primary PCI Function
Cisco IronPort Email Security	DLP
Cisco Physical Access Control	9.1
Cisco UCS and UCS Express	Servers
Cisco Unified CM and IP Phones	9.1.2
Cisco Video Surveillance	9.1.1

Administration	Primary PCI Function
Cisco ACS	7.1
Cisco Identity Services Engine	7.1, 11.1b, 11.1d
Cisco Prime LMS	1.2.2
Cisco Security Manager	1.2
Hytrust Appliance	10.5
RSA Authentication Manager	8.3
RSA Data Protection Manager	3.5
RSA enVision	10.5

Infrastructure	Primary PCI Function
Cisco ASA-Branch	1.3, 11.4
Cisco ASA-Data Center	1.3, 11.4
Cisco Branch Routers	1.3, 11.4
Cisco Branch Switches	Segmentation
Cisco Data Center Routers	1.2, 1.3
Cisco Data Center Switches	Segmentation
Cisco Data Center IDSM	11.4
Cisco MDS Switches	3.4
Cisco Nexus 1000V Series Switch	Segmentation
Cisco Nexus Data Center Switches	Segmentation
Cisco Nexus VSG	Virtual Firewall
Cisco Wireless	4.1, 11.1
EMC CLARiioN SAN	Storage



CHAPTER 5

Component Assessment

This chapter discusses the function of each component and how it helps to address PCI DSS 2.0 compliance requirements. Each component was assessed by Verizon Business, and the full reference architecture report is available in Appendix C, "Verizon Business Reference Architecture Report—Cisco PCI Solution."

This assessment took place at a specific point in time using currently available versions of products and software.

Component Section Overview

Each component section includes the following:

- Description
- PCI assessment summary
- Primary PCI function
- Capability assessment
- Design considerations
- PCI assessment detail

PCI Assessment Summary

For each component, the PCI Assessment Summary table (see Table 5-1) lists each of the PCI sub-requirements that were passed, required compensating controls, or failed.

Table 5-1 PCI Assessment Summary Example

Models Assessed	
Cisco Catalyst Switch	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3

Table 5-1 PCI Assessment Summary Example (continued)

PCI 6	6.1
PCI 7	7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Capability Assessment

Each component requires specific capabilities to be deployable in a compliant environment. Customers and vendors alike have complained that it is difficult to understand what capabilities are required when developing or purchasing equipment for the purpose of compliance. Therefore, Cisco has developed a simplified approach to clarify the scales that are relevant. Sub-requirements have been grouped for ease of assessment, as shown in Table 5-2.

Table 5-2 Capability Assessment Example

Cisco Component

PRIMARY FUNCTION
[Description of primary PCI function]
REQUIREMENT: [PCI requirement addressed]

cisco QSA Validated

PCI Security Standards Council PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

The PCI DSS 2.0 security standard is written from the perspective of helping an organization become compliant. It is not grouped in a clear manner for the evaluation of hardware or software. The following grouping of sub-requirements is an extrapolation of the standard to simplify the assessment of hardware and software:

- *Secure services* comprises sub-requirements that affect the secure administration and hardening of the component, and include the following:
  - Disable any unnecessary services—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers*. (Sub-requirements 2.2.2, 2.2.4)
  - Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)
  - Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)
- *Authentication* comprises sub-requirements that affect the identity of personnel accessing systems in the cardholder data environment, including the following:
  - Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed*. (Sub-requirement 7.1, 7.2)
  - Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data. Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
- *Logs* comprises sub-requirements that affect the forensic analysis capabilities of the cardholder data environment, including the following:
  - Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)
  - The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources*. (Sub-requirements 10.4.2, 10.4.3)

Table 5-3 explains the color-coded icons used in the tables.

Table 5-3 Color-Coded Icon Definitions

Icon	Description
	The component has the native capability to satisfy the requirement.
	The component has the capability to use other components to satisfy the requirement.
	The component requires compensating controls to satisfy the requirement.
	The component has no capability to satisfy the requirement.

Design Considerations

This section provides compliance principles as well as best practices for each technology deployed within an enterprise environment.

PCI Assessment Detail

This section includes the following:

- PCI sub-requirements satisfied by solution component—Lists which PCI sub-requirements were successfully audited and validated by the respective technology. Each sub-requirement includes a configuration example or reference of how the sub-requirement was met. This result is directly correlated to the implementation built in the Cisco lab and presented in Chapter 4, "Implementing and Configuring the Solution."
- PCI sub-requirements that require compensating controls—Lists which PCI sub-requirements needed additional compensating controls to successfully pass the PCI audit. Examples include additional configurations, products, or policies to meet compliance requirements.
- PCI sub-requirements that failed—Lists which PCI sub-requirements could not be satisfied.

Endpoints

The endpoints layer of the solution framework addresses the components such as voice, e-mail, and physical security.

Voice

Cisco Unified Communications Manager and IP Phones

The Cisco Unified Communication Manager is a suite of voice applications, signaling control, and utilities that provide IP communications capabilities using devices such as the IP phones. It is configured as an appliance that is easy to deploy, flexible to manage, and allows robust security.

Table 5-4 PCI Assessment Summary—Cisco Unified Communications Manager

Models Assessed	
Cisco Unified Communication Manager 8.5.1	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 9	9.1.2
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5

Table 5-4 PCI Assessment Summary—Cisco Unified Communications Manager (continued)

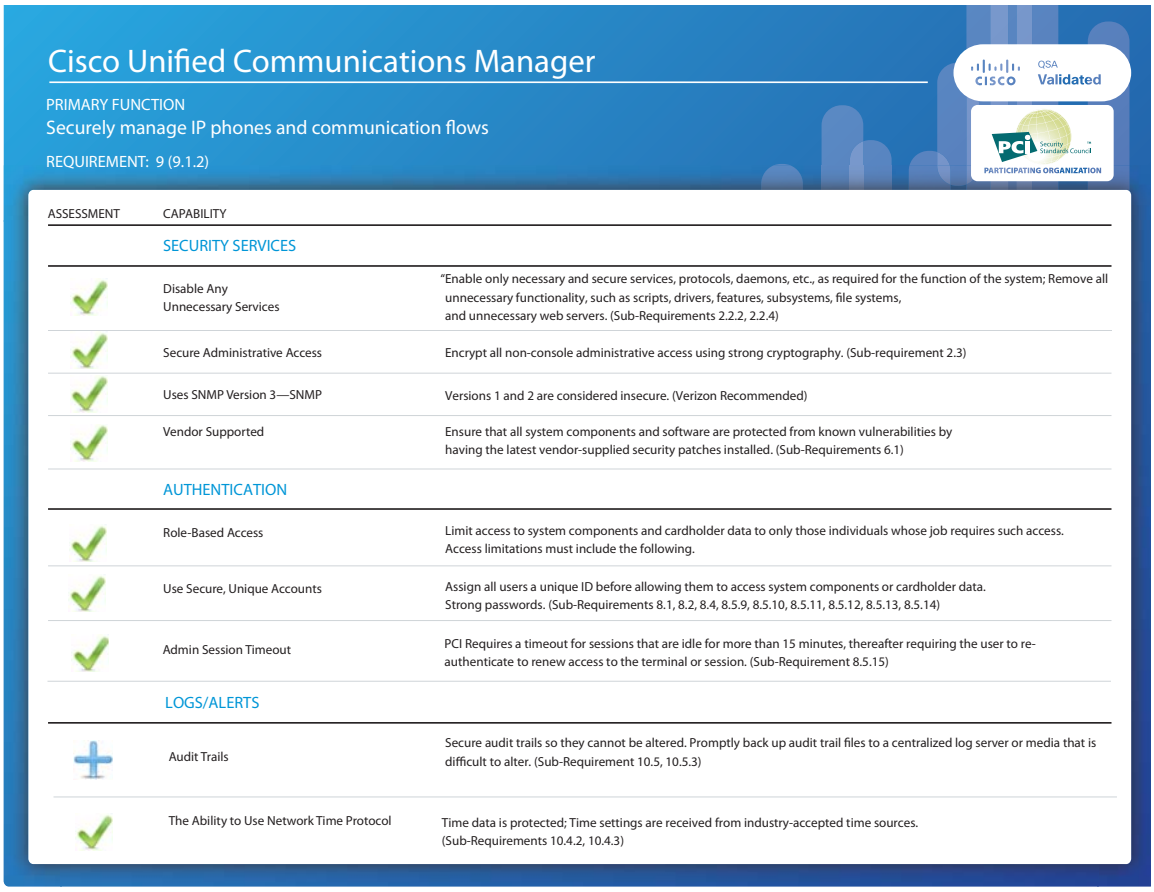
PCI Sub-Requirements Requiring Compensating Controls
No compensating controls were required to satisfy any sub-requirements.
PCI Sub-Requirements Failed
No sub-requirements were failed.

Primary PCI Function

The primary PCI function of Cisco Unified Communications Manager is to securely manage IP phones and communications flows, as well as securing publicly accessible network jacks (9.1.2).

Table 5-5 lists the component assessment details for Cisco Unified Communications Manager.

Table 5-5 Component Capability Assessment—Cisco Unified Communications Manager



Cisco Unified Communications Manager

PRIMARY FUNCTION
Securely manage IP phones and communication flows

REQUIREMENT: 9 (9.1.2)

cisco QSA Validated

PCI Security Standards Council PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
✓	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
✓	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

The design features for improving security for the Cisco Unified Communications Manager appliance include:

- Deployment as a clustered redundancy model that includes a publisher server and several subscriber servers
- Downloading and installing security patches when vulnerabilities are announced by the Cisco Product Security Incident Response Team (PSIRT)
- Implementing Transport Layer Security (TLS) messaging for secure signaling and Secure RTP (SRTP) for encrypted media throughout the enterprise
- Enabling device authentication and communication encryption using X.509 certificates that are signed by the Certificate Authority Proxy Function (CAPF) feature on the server

Best practices for Cisco Unified Communications Manager phone security are as follows:

- The Gratuitous ARP setting on the Cisco Unified IP Phones should be disabled.
- Disabling the web access setting prevents the phone from opening the HTTP port 80; this blocks access to the phone's internal web pages.
- Disabling the PC Voice VLAN access setting in the phone configuration window prevents the devices connected to the PC port from using the voice VLAN functionality.
- Disabling the Setting Access option in the phone configuration window prevents users from viewing and changing the phone options, including the Network Configuration options, directly on the phone.
- Cisco Unified IP Phones can be configured for authentication and encryption by installing a CTL file on the phones that includes security tokens, trusted server and firewall information, and CAPF.

For more information on securing Unified Communications, see the *Cisco Unified Communications System 8.x SRND* at the following URL:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/security.html

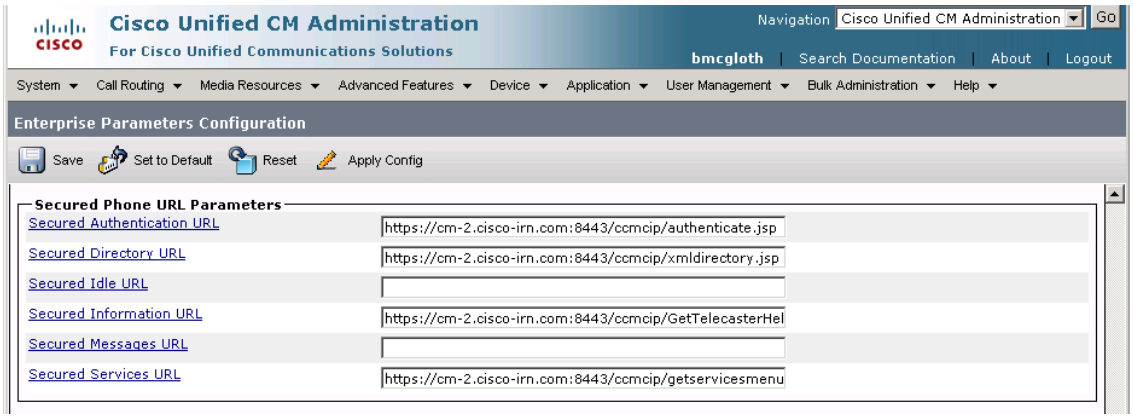
PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The Cisco Unified Communication Manager appliance operating system includes only the components needed to run the application. Root access to the OS is disabled and this prevents any unwanted services from being implemented. Telnet and HTTP access to the server administration is disabled. The communication between phones and server over HTTP can be secured using SSL. (See Figure 5-1.)

Figure 5-1 Enterprise Parameters Configuration



- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco Unified Communication Manager appliance does not allow changes to the operating system, or to the database or installation of unsupported hardware or of unsupported third-party software.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The Cisco Unified Communication Manager uses SSL for web-based administrative and user access and uses SSH for remote terminal access.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team (PSIRT) site tracks and publishes information about any relevant exposures and vulnerabilities in the Cisco Unified Communication Manager appliance. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise through a web browser or CLI.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

  For more information about PSIRT, see the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

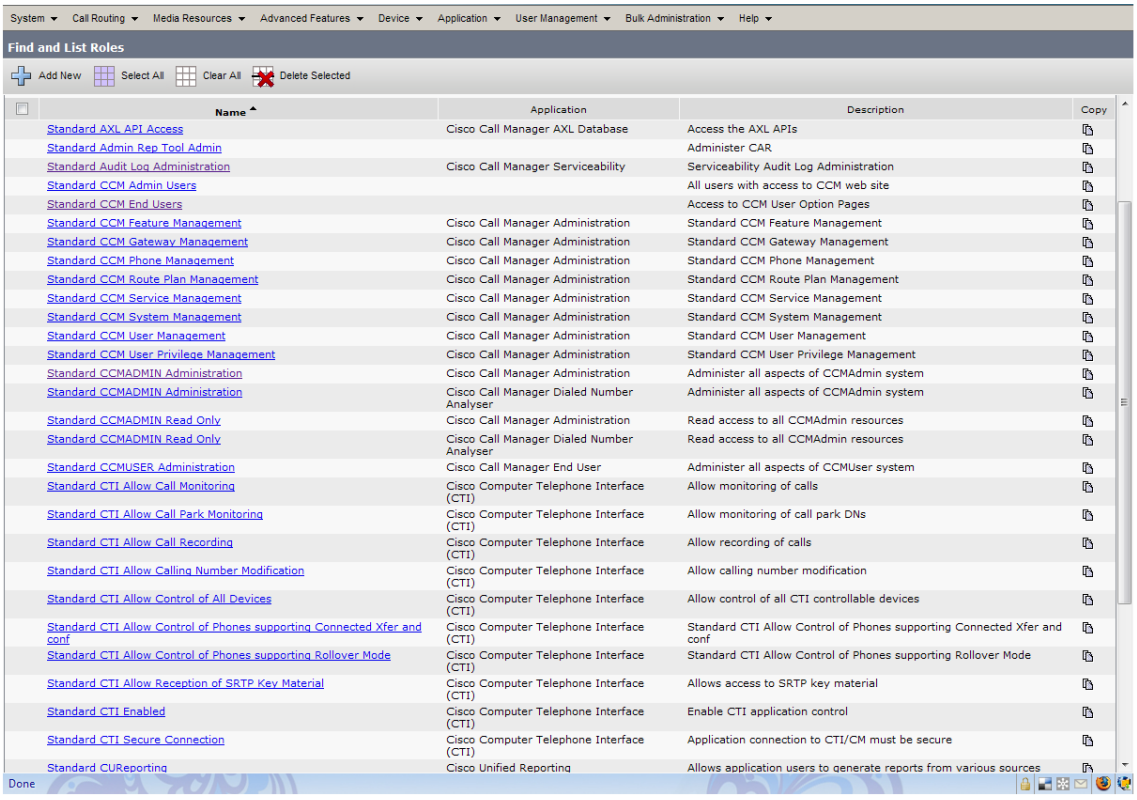
Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the Cisco Unified Communication Manager's internal database. Cisco Unified Communication Manager also supports linking to a centralized user database such as Active Directory using LDAP. Within Cisco Unified Communication Manager, individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

  The Cisco Unified Communication Manager uses various role definitions for permitting access to various application components on the server. (See Figure 5-2.)

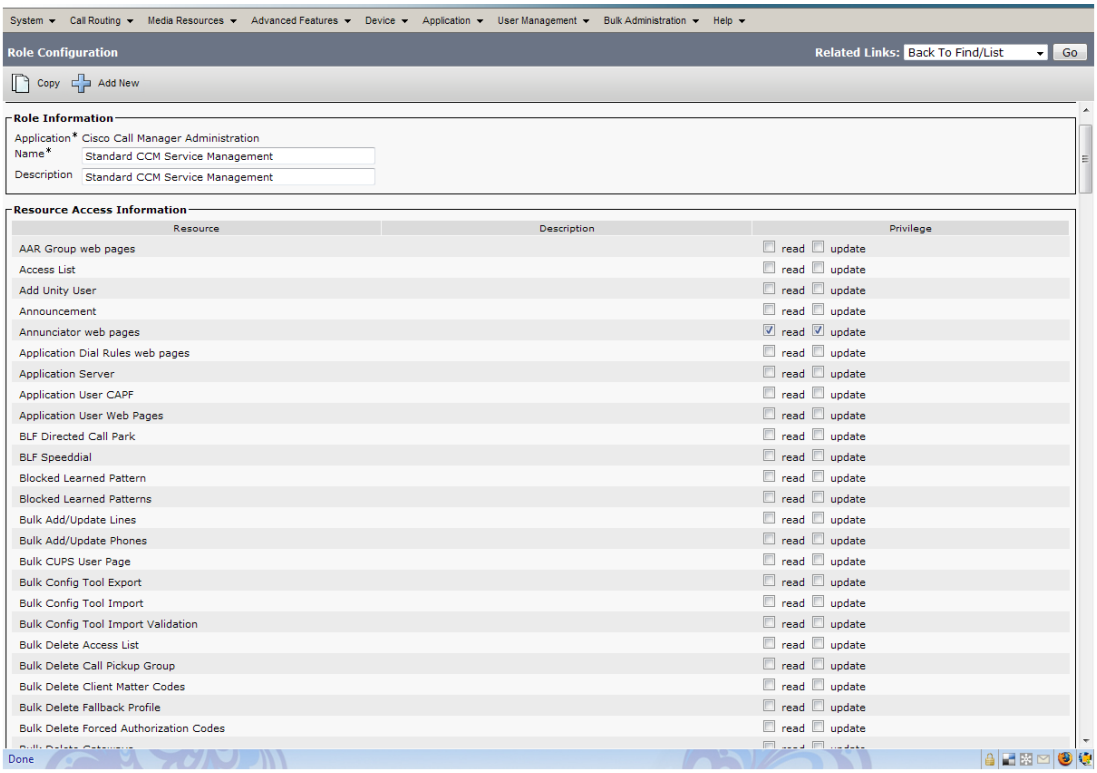
Figure 5-2 Find and List Roles



- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

The role configuration menu in the Cisco Unified Communication Manager server allows specifying the assignment of privileges based on the role description. No systems access is permitted without an account. (See Figure 5-3.)

Figure 5-3 Role Configuration



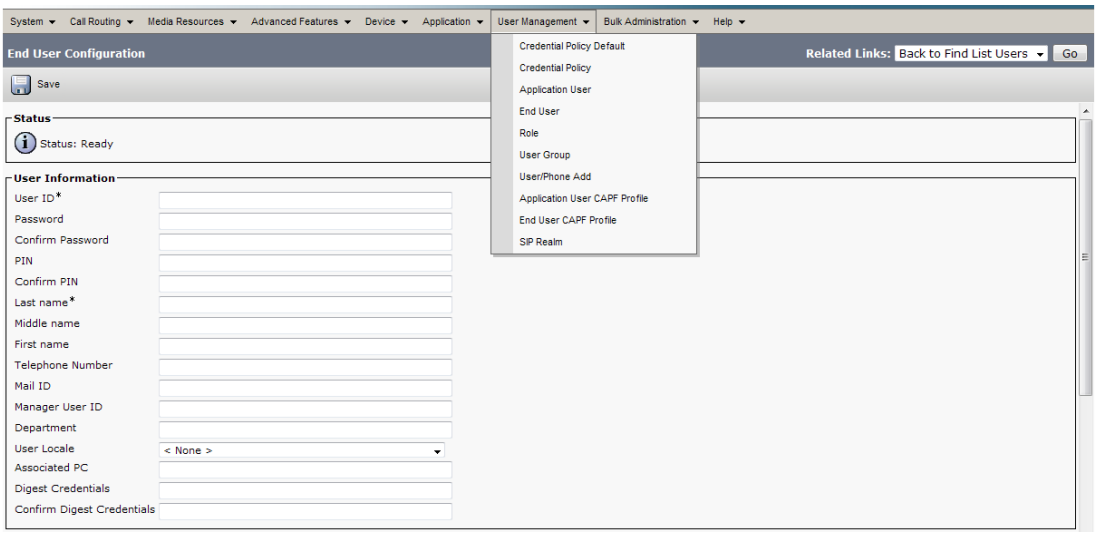
Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database, as shown below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Sub-requirements 8.1, 8.2, and 8.4 are met by configuring user IDs and passwords in the User Management section of the Cisco Unified Communication manager web interface, as shown in Figure 5-4.

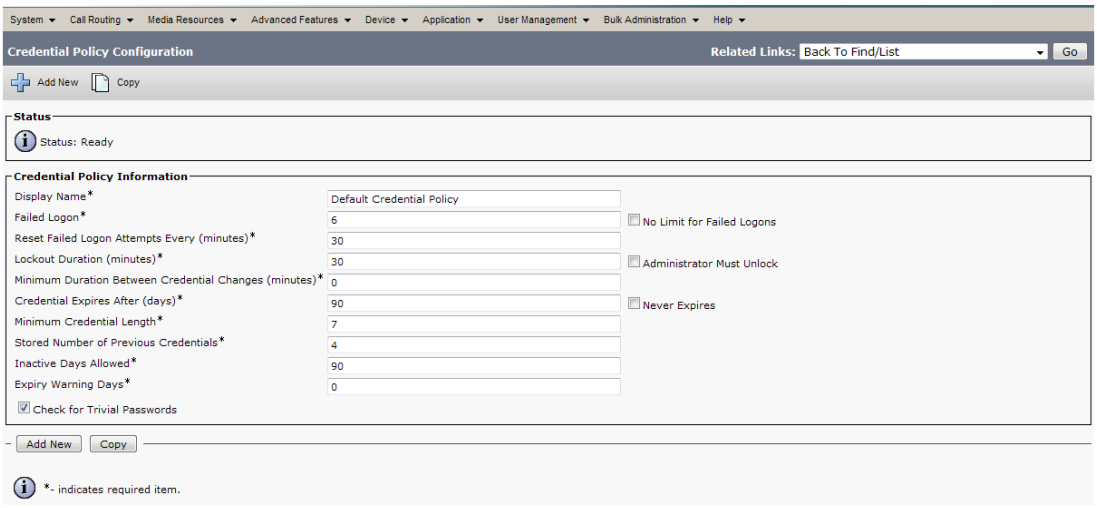
Figure 5-4 End User Configuration



- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Sub-requirements 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, and 8.5.14 are met by configuring a credential policy for user management and applying that policy to a designated group. Figure 5-5 shows a modified default credential policy.

Figure 5-5 User Credential Policy Configuration



Check for Trivial Passwords	Check this check box to require the system to disallow credential that are easily hacked, such as common words, repeated character patterns, and so on. The default setting checks the check box.

290984

The system provides trivial credential checks to disallow credentials that are easily hacked. You enable trivial credential checks by checking the Check for Trivial Passwords check box in the Credential Policy Configuration window.

Passwords can contain any alphanumeric ASCII character and all ASCII special characters. A non-trivial password meets the following criteria:

- Must contain three of the four allowable characteristics: uppercase character, lowercase character, number, and symbol.
- Must not use a character or number more than three times consecutively.
- Must not repeat or include the alias, username, or extension.
- Cannot consist of consecutive characters or numbers (for example, passwords such as 654321 or ABCDEFG)

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

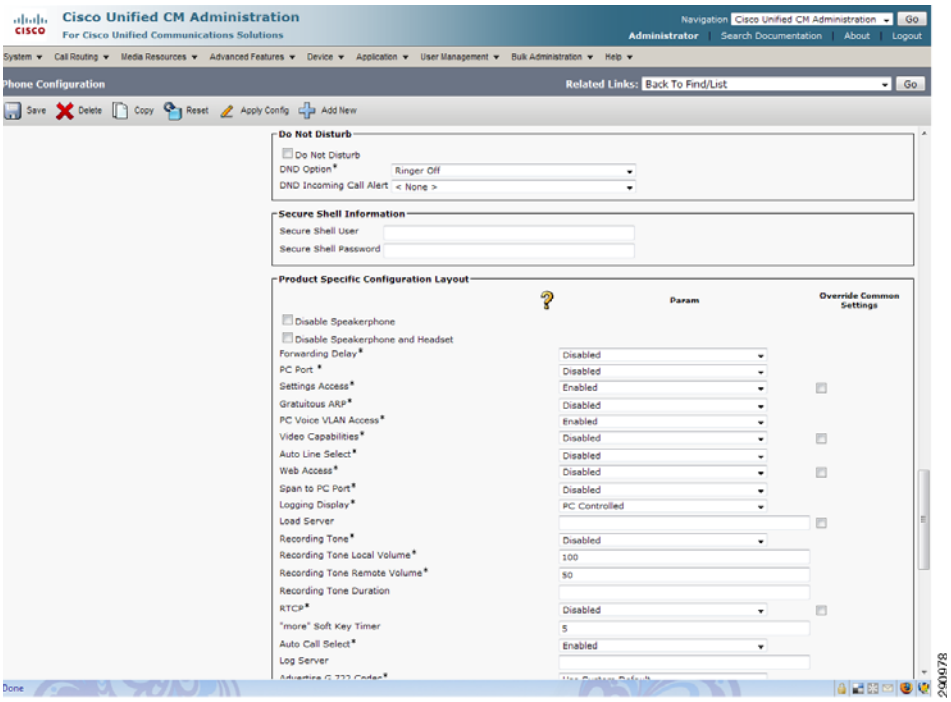
  Sub-requirement 8.5.15 is part of the default system behavior. The system locks the user's session if the session has been idle for fifteen minutes, requiring the user to login again.

Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.2**—*Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.*

  This requirement is met by disabling the PC port setting in the phone configuration window for ports that are not in use, as shown in Figure 5-6.

Figure 5-6 Phone Configuration



Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco Unified Communications Manager is able to track and monitor all administrative user access and events.

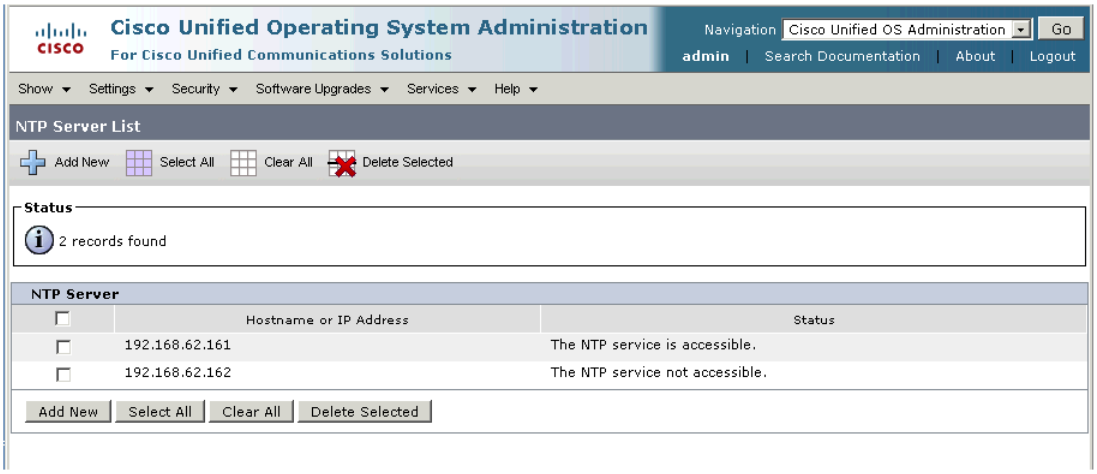
- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Unified Communication manager uses Network Time Protocol (NTP) to update and synchronize local clock facilities to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. This requirement is met by configuring the NTP server, as shown in Figure 5-7.

Figure 5-7 NTP Server List



To meet all of the requirements listed below, the PCI solution uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  The Cisco Unified Communication Manager can be configured to send the logs to an external syslog server where it cannot be altered by the appliance users. Figure 5-8 and Figure 5-9 show the configurations necessary for log forwarding.

Figure 5-8 Enterprise Parameters Configuration

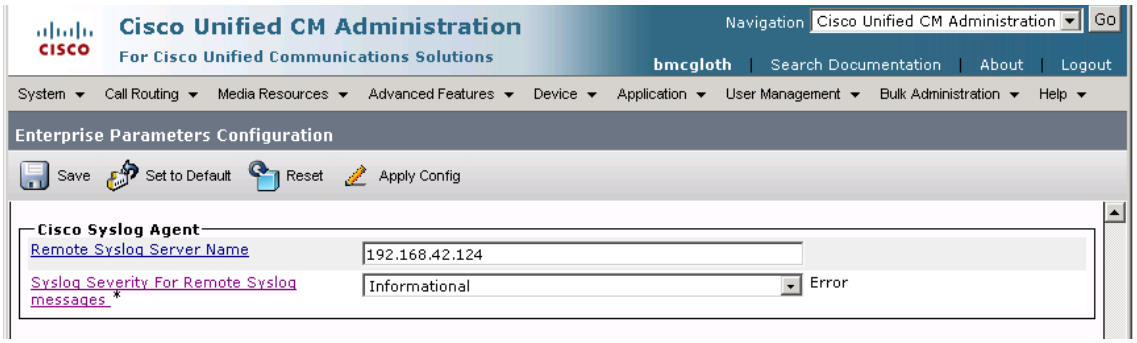
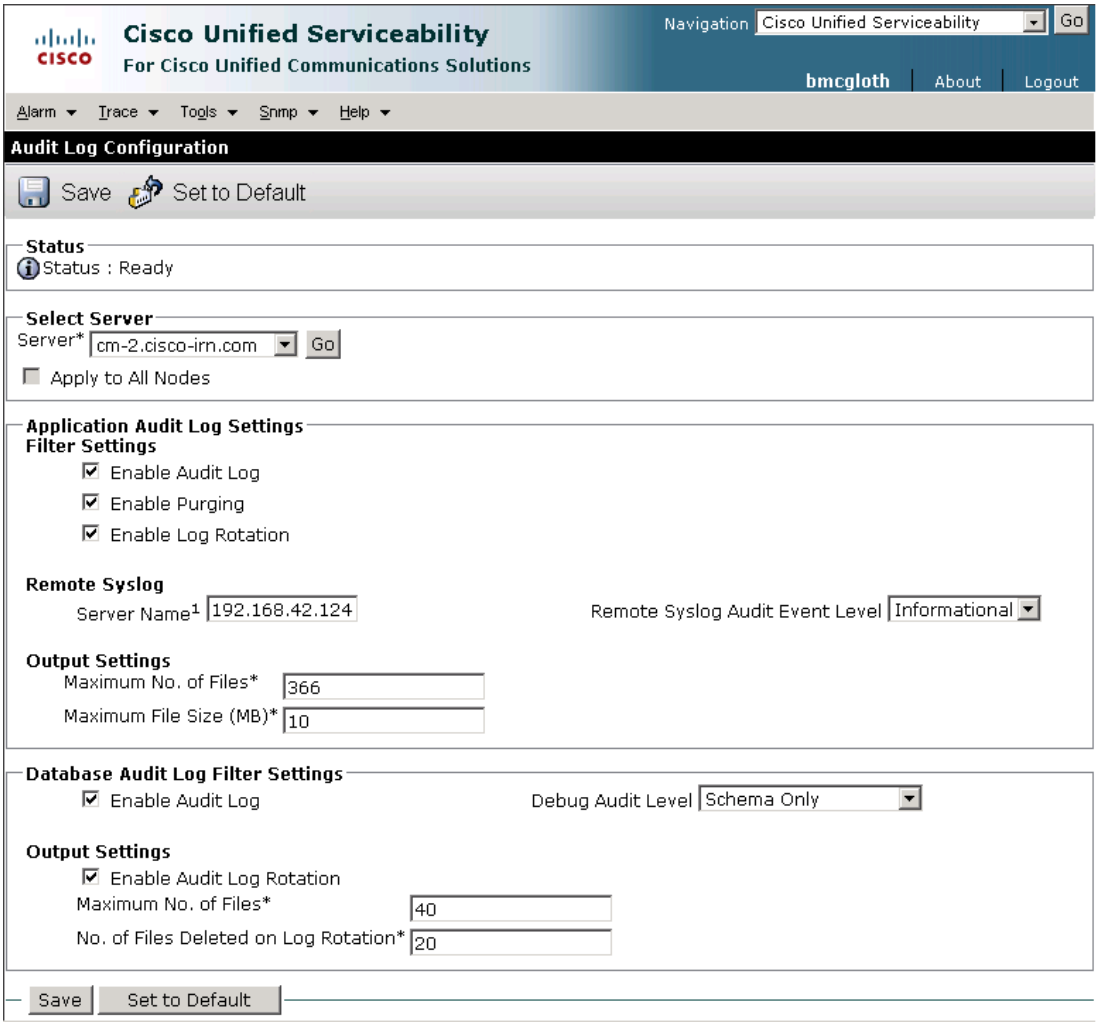


Figure 5-9 shows the necessary configuration under Cisco Unified Serviceability.

Figure 5-9 Audit Log Configuration



PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Physical Security

Cisco Physical Security solutions provide broad capabilities in video surveillance, IP cameras, electronic access control, and groundbreaking technology that converges voice, data, and physical security in one modular platform. Cisco Physical Security solutions enable customers to use the IP network as an open platform to build more collaborative and integrated physical security systems while preserving their existing investments in analog-based technology. As customers converge physical security infrastructures and operations and begin using the IP network as the platform, they can gain significant value through rapid access to relevant information and interoperability between systems. This creates a higher level of situational awareness and allows intelligent decisions to be made more quickly.

Cisco Video Surveillance

Video surveillance technology provides security monitoring capabilities within a branch and data center environment. Video surveillance for loss prevention can now be extended into the area of protecting the cardholder data environment.

As the core component of Cisco's video surveillance software portfolio, the Cisco Video Surveillance Media Server offers the power and flexibility to meet a diverse range of video surveillance requirements. The media server:

- Uses IP technology to provide outstanding scalability in terms of sites, cameras, viewers, and storage
- Delivers low-latency, high-quality, event-tagged video
- Supports a broad range of cameras, codecs (such as JPEG, and MPEG-4, and H.264), viewing platforms, and network topologies
- Archives at various frame rates, durations, and locations

Quickly and effectively configure and manage video throughout your enterprise with the Cisco Video Surveillance Operations Manager (VSOM). Working in conjunction with the Cisco Video Surveillance Media Server and Cisco Video Surveillance Virtual Matrix, the Operations Manager meets the diverse needs of administrators, systems integrators, and operators by providing:

- A web-based toolkit for configuration, management, display, and control of video from a wide variety of both Cisco and third-party surveillance endpoints
- Management of a large number of Cisco Video Surveillance Media Servers, Virtual Matrixes, cameras, and users
- Flexible video recording options including motion-based, scheduled, and event-based
- Comprehensive control of users and user roles including scheduling of operator shifts, event filters, and user-specific video views
- Detailed activity reports and system audit

Table 5-6 PCI Assessment Summary—Cisco Video Surveillance

Models Assessed	
Cisco Video Surveillance Manager version 6.3.1	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 9	9.1, 9.1.1
PCI 10	10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 104.3, 10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function of video surveillance is to monitor physical access to sensitive areas within the cardholder data environment (9.1.1).

Table 5-7 lists the component assessment details for the Cisco Video Surveillance solution.

Table 5-7 Component Capability Assessment—Cisco Video Surveillance



Cisco Video Surveillance

PRIMARY FUNCTION
Monitor physical access to sensitive areas within the cardholder environment

REQUIREMENT: 9 (9.1.1)

QSA Validated

PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
✓	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Ensure that cameras are positioned to monitor servers or systems within the cardholder data environment.
- Cameras should be appropriately positioned to identify personnel accessing these systems.
- Ensure adequate storage of video for three months.

For more information, see the Cisco IP Video Surveillance Guide at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVSchap4.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2—***Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The Cisco Video Surveillance Manager includes only the required services, ports, applications, and access required for standard operation of the system. Use the Cisco Video Surveillance Operations Manager Secure Login feature, found within the Administrative Settings, to enable and force secure HTTPS application login.

- **PCI 2.2.4—***Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco Video Surveillance Manager and Multiservices Platform contain only the required components needed to run the applications. If additional network, software, or platform security customization is required, consult *Securing Video Surveillance Manager: Best Practices and Recommendations* at the following URL:
  http://www.cisco.com/en/US/docs/security/physical_security/video_surveillance/network/design/bestprac_4_1_6_1.pdf

- **PCI 2.3—***Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The Cisco Video Surveillance Manager uses SSL for web-based administration and operator access, and uses SSH for remote terminal access. Use the Cisco Video Surveillance Operations Manager Secure Login feature, found within the Administrative Settings, to enable and force secure HTTPS application login. SSH access should be used to securely login to the VSM host.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team (PSIRT) site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Video Surveillance Operations Manager. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

  For more information about PSIRT, see the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of requirement 7 were met using VSOM's Role-based Access Control (RBAC) system to logically group each user within a role based on their need to know. This restricts unauthorized access and usage of system components. The VSOM RBAC allows granular access control for each system component, including devices such as servers, cameras, and encoders, along with application-level functionality of accessing these resources.

This configuration was used to address the following individual requirements.

- **PCI 7.1—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:*
  - **PCI 7.1.1—***Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
  - **PCI 7.1.2—***Assignment of privileges is based on individual personnel's job classification and function*

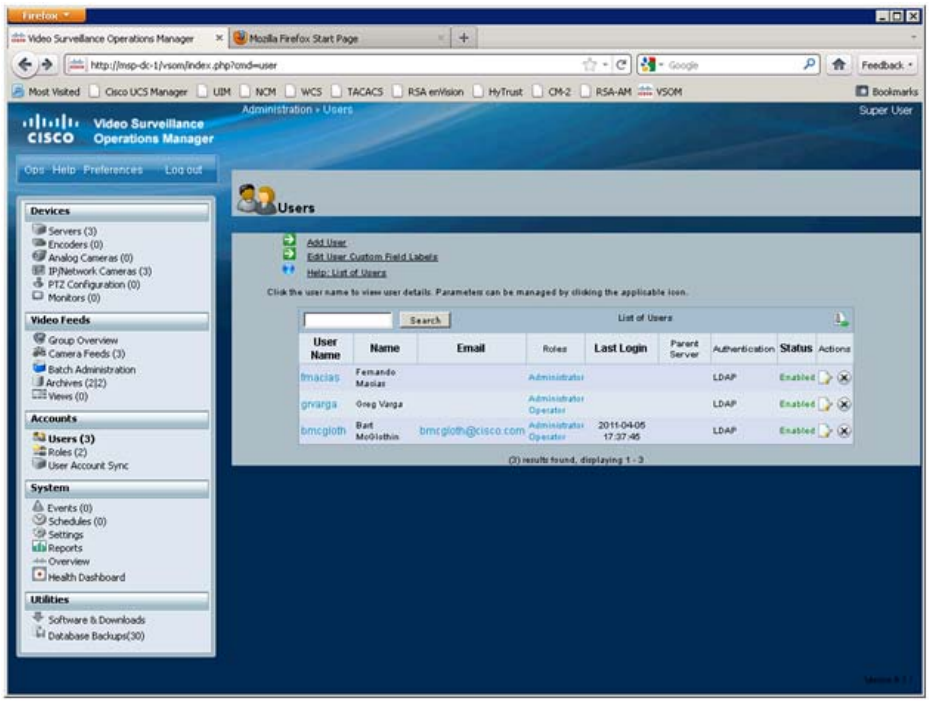
  - **PCI 7.1.3—***Requirement for a documented approval by authorized parties specifying required privileges.*
  - **PCI 7.1.4—***Implementation of an automated access control system*

- **PCI 7.2—***Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:*
  - **PCI 7.2.1—***Coverage of all system components*
  - **PCI 7.2.2—***Assignment of privileges to individuals based on job classification and function*
  - **PCI 7.2.3—***Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  The role configuration menu in Video Surveillance Operations Manager server allows specifying the assignment of privileges based on the role description. No systems access is permitted without an account.

  Individual users and roles are created locally and authentication directed to LDAP, as shown in Figure 5-10.

Figure 5-10 VSOM Users Authenticate to LDAP Service



Requirement 8: Assign a Unique ID to Each Person with Computer Access

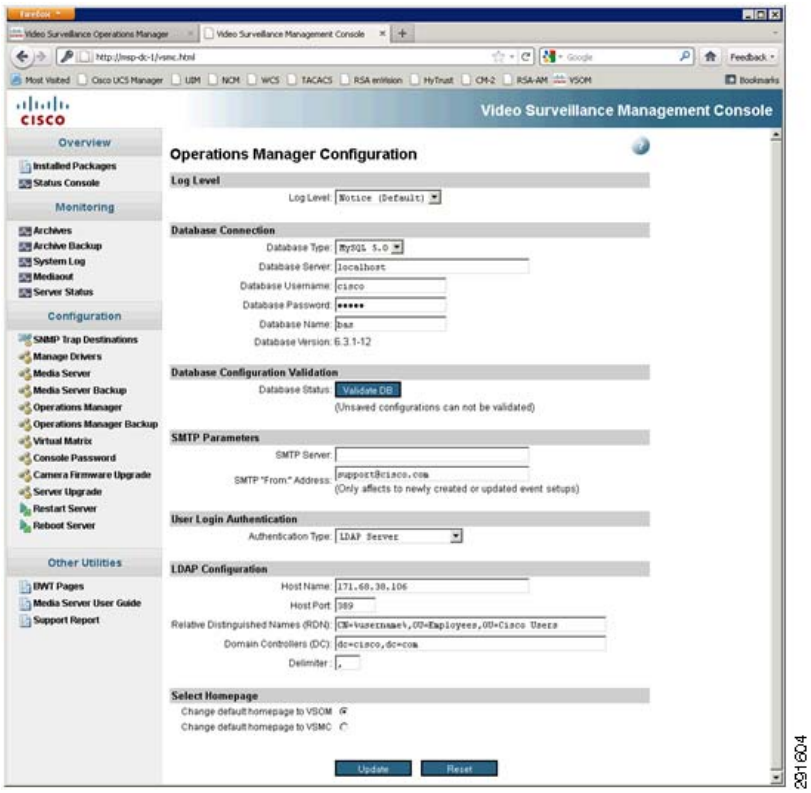
Compliance of the sub-requirements in this section was achieved within the solution by implementing LDAP connectivity for AAA services and Microsoft Active Directory for user account services. Configure AAA services via LDAP, as shown below.

- **PCI 8.1—***Assign all users a unique ID before allowing them to access system components or cardholder data.*

- **PCI 8.2—***In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4—***Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5—***Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9—***Change user passwords at least every 90 days.*
- **PCI 8.5.10—***Require a minimum password length of at least seven characters.*
- **PCI 8.5.11—***Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12—***Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13—***Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14—***Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Using the Video Surveillance Management Console, configure LDAP as specified in the installation guide. Figure 5-11 shows the LDAP configuration implemented for validation.

Figure 5-11 VSOM LDAP Configuration



- **PCI 8.5.15—***If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco VSOM has a minimum session timeout of 30 minutes in the configuration for the version validated. Administration time limits would need to be enabled systemically through an active directory policy to the admin workstation desktops, locking them when there is no activity after 15 minutes.

Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1—***Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.*
- **PCI 9.1.1—***Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a branch.*

  Physical access to sensitive areas and cardholder data is restricted by solutions in video surveillance management and IP cameras by securing data center facilities and cashier areas within branches. This includes video recording options for flexible configuration of video recording archives and low-latency, high-quality, event-tagged video. Also available is the following:

  - A web-based interface for configuration, management, display, and control of video from a wide variety of surveillance and monitoring endpoints
  - Management of a large number of video surveillance media servers, video walls, cameras, and users
  - Comprehensive control of users and user roles including scheduling of operator shifts, event filters, and user-specific video views
  - Detailed activity reports and system audit

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco VSOM is able to track and monitor all administrative user access and events.

Cisco VSOM uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*

  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*
- **PCI 10.4—***Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).*
  - **PCI 10.4.2—***Time data is protected.*
  - **PCI 10.4.3—***Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Network Time Protocol (NTP) is supported and must be enabled within both the IP cameras and Video Surveillance Manager.

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects information from all devices to ensure the integrity and correlation of events.

Requirement 10.5 was met using the integrated Log Backup functionality to send the logging data to the RSA enVision server.

- **PCI 10.5—***Secure audit trails so they cannot be altered.*
  - **PCI 10.5.1—***Limit viewing of audit trails to those with a job-related need.*
  - **PCI 10.5.2—***Protect audit trail files from unauthorized modifications.*
  - **PCI 10.5.3—***Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
  - **PCI 10.5.5—***Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  The following configuration script was implemented to send the local log files to the RSA enVision server to be secured and the integrity established:

```
Directory:  /etc/cron.daily
Filename:  ftp-backup-files.cron

#!/bin/sh
FTP_USER=anonymous
FTP_PASS='vsom@cisco.com'
localDIR="/usr/BWhttpd/bas/db/backups"
serverDIR="/vsom_backup/"

cd $localDIR
ftp -n -i 192.168.42.124   <<EOF
user $FTP_USER $FTP_PASS
binary
cd $serverDIR
mput VSOM_MSP-DC-1_backup_20$(date +%y%m%d)*.tar.gz
quit
EOF
```

```
exit 0
```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

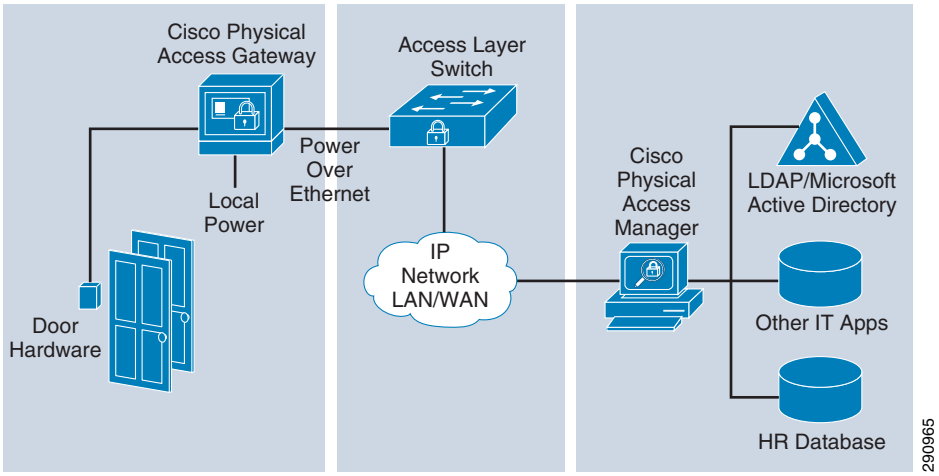
Cisco Physical Access Control

Cisco Physical Access Control allows organizations to secure their physical doors and locations. Cisco Physical Access Control addresses specific PCI requirements by providing:

- Secure access to the server by supporting secure protocols such as HTTPS and also securing the accounts using strong passwords
- Role-based access to the system by making use of profiles that can restrict access to the modules, depending on the roles
- Automated backup of events to a centralized server
- Ability to archive audit reports on a centralized server

Cisco Physical Access Control is a comprehensive IP-based solution that uses the IP network as a platform for integrated security operations (see Figure 5-12). It works with existing card readers, locks, and biometric devices and is integrated with Cisco Video Surveillance Manager (VSM) and with Cisco IP Interoperability and Collaboration System (IPICS).

Figure 5-12 Scalable, Modular Architecture



Cisco Physical Access Control has two components:

- The hardware component, Cisco Physical Access Gateway, provides a modular and scalable platform to connect readers, inputs, and outputs to the system. The gateway scales from a single door to thousands of doors at a fixed cost per door.
- The software component, Cisco Physical Access Manager, manages the hardware, monitors activity, enrolls users, and integrates with IT applications and data stores.

Table 5-8 PCI Assessment Summary—Cisco Physical Access Manager

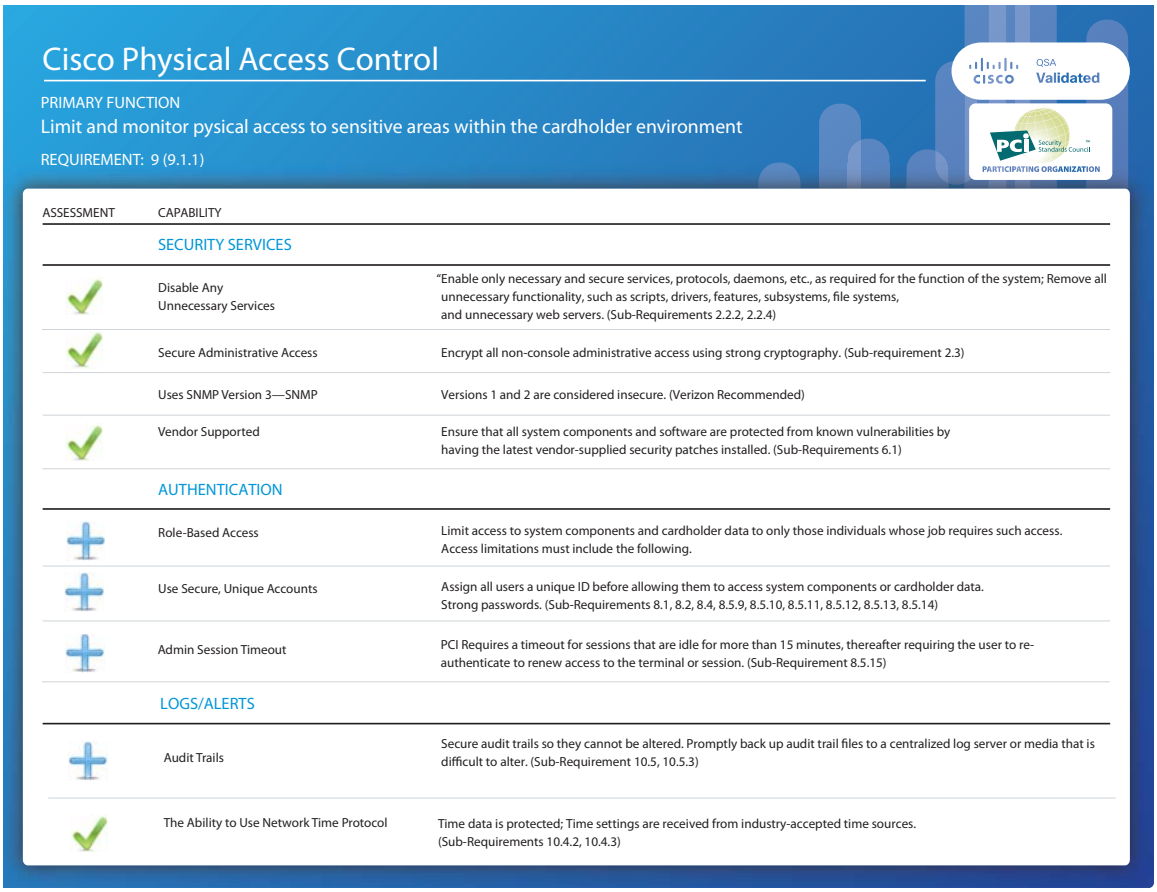
Models Assessed	
Cisco Physical Access Manager version 1.2.0	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function of the CPAM appliance is to configure, manage, monitor, and report on the physical doors and door hardware, protecting sensitive areas within the cardholder data environment (9.1).

Table 5-9 lists the component assessment details for Cisco Physical Access Control.

Table 5-9 Component Capability Assessment—Cisco Physical Access Control



Cisco Physical Access Control

PRIMARY FUNCTION

Limit and monitor pysical access to sensitive areas within the cardholder environment

REQUIREMENT: 9 (9.1.1)

QSA Validated

PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

Best practices are as follows:

- Use high availability for Cisco Physical Access Manager (PAM) servers.
- Map each branch location and identify the following:
  - Actual doors and modules
  - Door devices and module ports
- Use backup power supply for servers, modules, and devices.
- Cisco PAM was implemented following the Cisco Physical Access Manager Appliance User Guide, Release 1.2.0: http://www.cisco.com/en/US/docs/security/physical_security/access_control/cpam/1_2_0/english/user_guide/cpam_1_2_0.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2—***Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The Cisco PAM appliance can be configured to disable unsecure protocols. To disable unsecure protocols, you must edit one of the configuration files on the Cisco PAM appliance. The step-by-step instructions are as follows:

  - SSH into the Cisco PAM server
  - sudo su
  - Enter the *cpamadmin* password
  - /etc/init.d/cpamadmin stop
  - Comment out a configuration from the file /opt/cisco/cpam/apache-tomcat/conf/server.xml.

  Remove or comment the snippet below.

```
<Connector executor="tomcatThreadPool"
           port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

```
/etc/init.d/cpamadmin start
```

  When you try to launch the web UI using HTTP, you see “Page cannot be displayed”.

- **PCI 2.2.4—***Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco PAM appliance operating system includes only the components needed to run the application.

- **PCI 2.3—***Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  On the Cisco PAM appliance, SSL is enabled by default. All the communication between the Cisco PAM client and the gateway is encrypted using the 128-bit AES encryption. Console access to Cisco PAM is through SSH.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco PAM. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT, see the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

To meet all of the requirements listed below, the PCI solution uses a centralized user database in the Active Directory, which is linked via LDAP, RADIUS, and TACACS+ services. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. Cisco Physical Access Manager connects to this resource via LDAP to address the following individual requirements:

- **PCI 7.1—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:*
  - **PCI 7.1.1—***Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
  - **PCI 7.1.2—***Assignment of privileges is based on individual personnel's job classification and function*
  - **PCI 7.1.3—***Requirement for a documented approval by authorized parties specifying required privileges.*
  - **PCI 7.1.4—***Implementation of an automated access control system*

  Role-based access can be configured on Cisco PAM by making use of profiles. Profiles are pre-defined sets of access privileges that define the Cisco PAM modules and commands available to a user. For example, users that should have all privileges can be assigned to the Administrators profile.

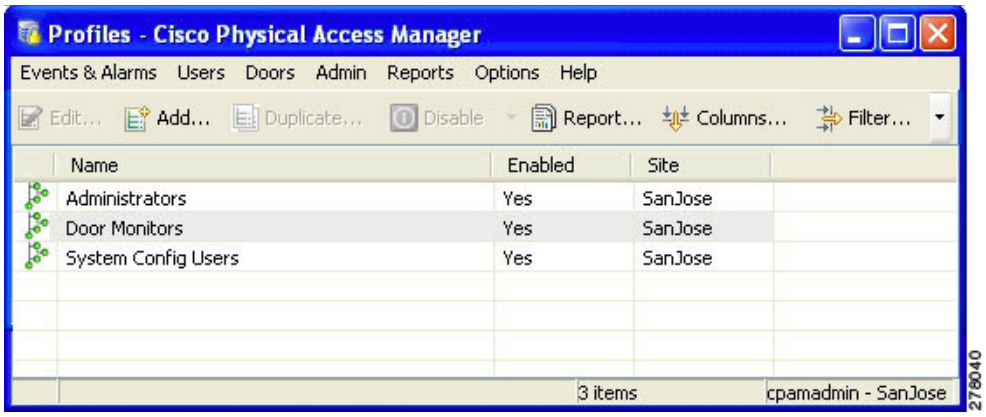
Note The Administrator profile is read-only and cannot be changed.

To create profiles, do the following:

Step 1 Select **Profiles** from the Users menu.

Step 2 To add a profile, choose **Add**. (See Figure 5-13.)

Figure 5-13 Profiles Module Main Window



Note To modify an existing profile, select the entry and choose **Edit**. To remove a profile, select the entry and choose **Delete**. The Administrator profile is read-only and cannot be changed.

Step 3 Select a Profile template that most closely matches the desired level of user access, as shown in Figure 5-14:

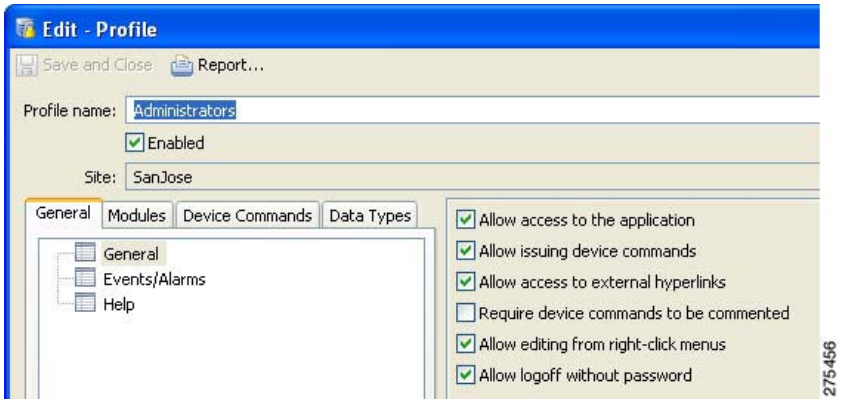
- Default—A basic set of privileges is set.
- Most Restrictive—No privileges are set.
- Least Restrictive—All privileges are set.

Figure 5-14 Profile Templates



Step 4 Enter the basic profile settings, as shown in Figure 5-15.

Figure 5-15 Profile—General Tab



- Profile name—Enter a descriptive name for the profile.

- Enabled—Select the check box to enable the profile, or deselect the box to disable the profile.
- Partition—Select the partition from the drop-down menu.

Step 5 Click the **General** tab to define the basic profile properties. Click the checkbox next to each field to enable or disable the privilege, as described in Table 5-10.

Table 5-10 General Settings—Profile Module

Field	Description
General	
Allow access to the application	Allows access to the application.
Allow issuing device commands	Allows user to issue device commands directly to hardware.
Allow access to external hyperlinks	Allows access to external hyperlinks.
Require device commands to be commented	Requires the user to enter a comment with each device command issued in the system.
Allow editing from right-click menus	Allows access to the right-click the Edit menu.
Allow logoff without password	Allows user to logoff without a password.
Events/Alarms: Alarm Annotations (Ack., Clear, Comment)	
Allow annotations	Allows user to acknowledge, clear, and comment alarms. Click the **Filter** button to define the events that trigger the action.
Allow multiple annotations	Allows the user to acknowledge, clear, and comment multiple alarms at one time.
Allow clearing of unacknowledged alarms	Allows the user to clear unacknowledged alarms from active devices.
Allow clearing of active device alarms	Allows the user to clear alarms from active devices.
Events/Alarms—On new alarms	
Open Alarms Module	The **Alarms** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Open Manage Alarm window	The **Alarms** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Open graphic map	The **Graphic Map** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show recorded video	Displays recorded video with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show live video	Displays live video with new system alarms. Click the **Filter** button to define the events that trigger the action.
Help—Defines access to the various help systems	
Allow access to help documentation	Allows access to help documentation.

Table 5-10 General Settings—Profile Module (continued)

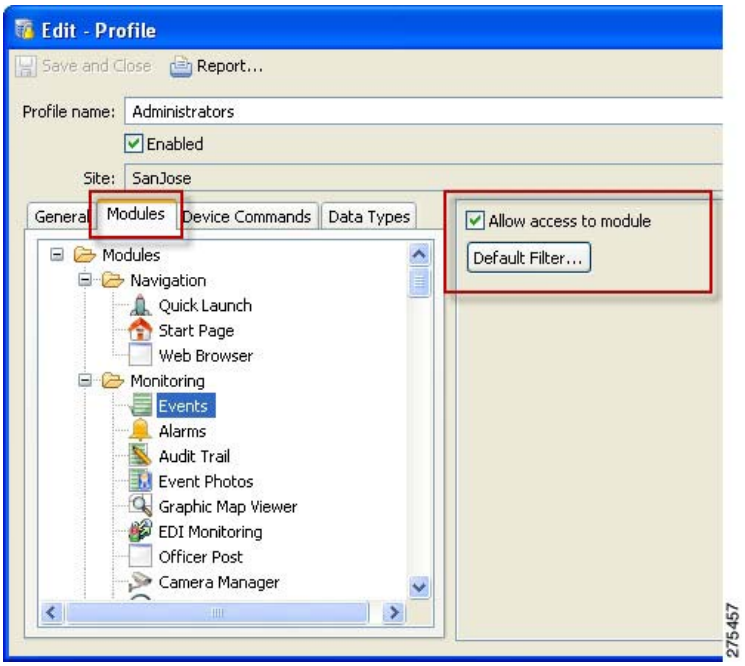
Enable context menu in help browser	Allows the user to view the help context menu.
Allow access to help PDF	Allows the user to access the help PDF. Adobe PDF viewer is required.

Step 6 Click the **Modules** tab to define the modules accessible to the profile, as shown in Figure 5-16.

a. Select a Cisco PAM module.

b. Select **Allow access to module** to enable access to the module.

Figure 5-16 Profile—Modules Tab



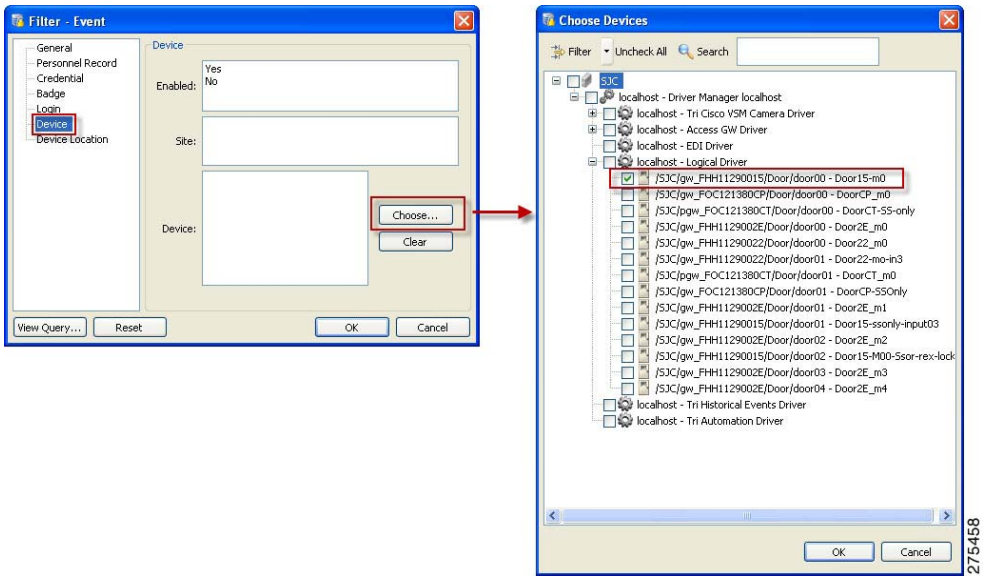
c. (Optional) Use the **Default Filter** with modules such as Event, Badge, and Personnel to define the filter applied when a user opens the module.

For example, to create a profile with access to the Events module that displays events for a specific door by default, complete the following sample steps:

1. Create a profile with access to the Events module, as described in the previous steps.
2. Click **Default Filter**, as shown in Figure 5-16.
3. Select the **Device** tab, as shown in Figure 5-17.
4. Click **Choose**.

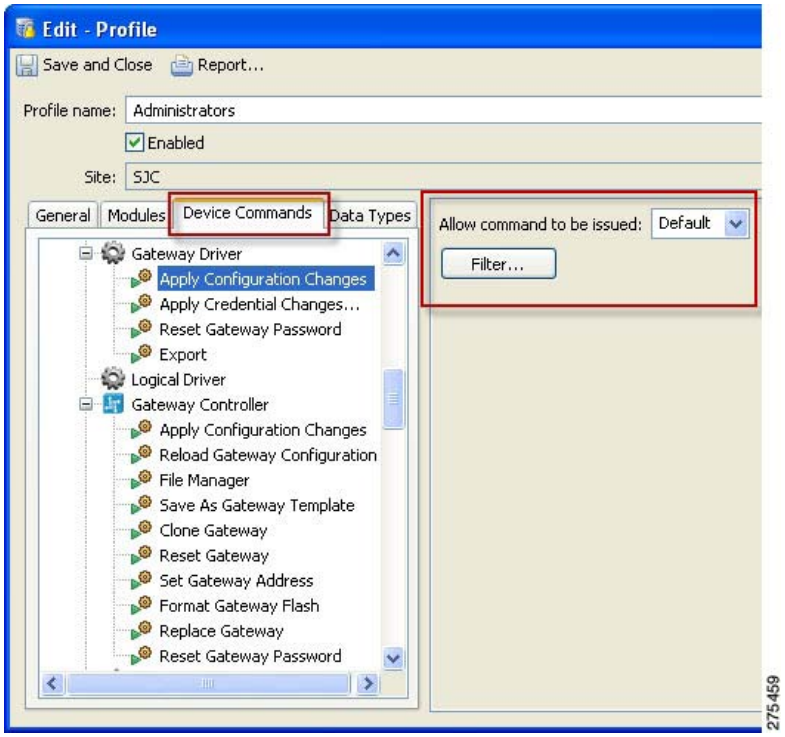
   In the Choose Devices window, expand the Logical Driver device tree and select a door (Figure 5-17).
5. Click **OK** to save the changes and close the windows.

Figure 5-17 Default Filter: Device Settings



Step 7 Click the **Device Commands** tab to define the hardware configuration commands available to the user (see Figure 5-18).

Figure 5-18 Profile—Device Commands Tab



a. Expand or collapse the list of commands for a device.

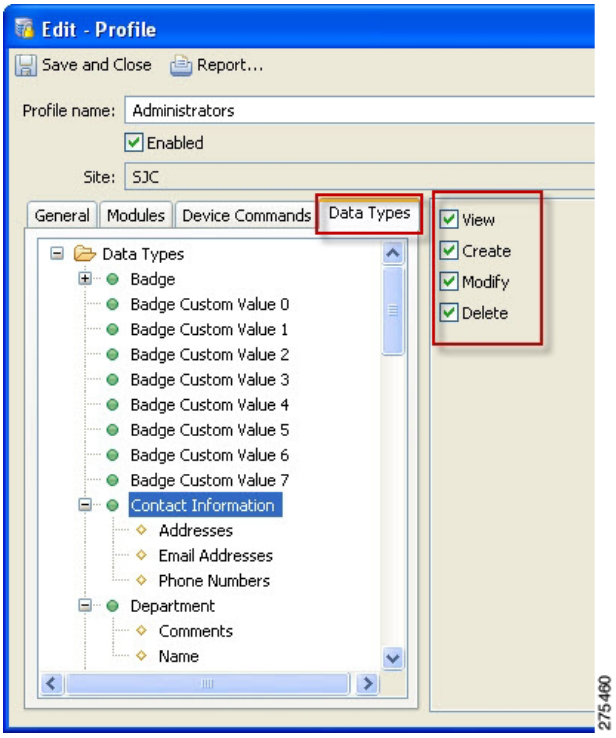
b. Highlight a command.

c. Select the following options:

- Allow command to be issued:
  - Default—If user has access to issue device commands, the command access is enabled by default.
  - No—Denies access to the command.
  - Yes—Allows access to the command.
- Filter—Apply a filter to limit the devices for the command.

Step 8 Click the **Data Types** tab to define the data available to the profile, as shown in Figure 5-19.

Figure 5-19 Profile—Data Types Tab



a. Select a module and the type of data in the list.

b. To restrict the data, click the check boxes for the properties listed in Table 5-11.

Table 5-11 Profile—Data Types

Field	Description
View	Allows the user to view the selected data type.
Create	Allows the user to add and create the selected data types.
Modify	Allows the user to modify existing data.
Delete	Allows the user to delete data.
Default Filter...	Allows the user to apply a default filter to limit objects from view.

Step 9 Click **Save and Close** to save the profile settings.

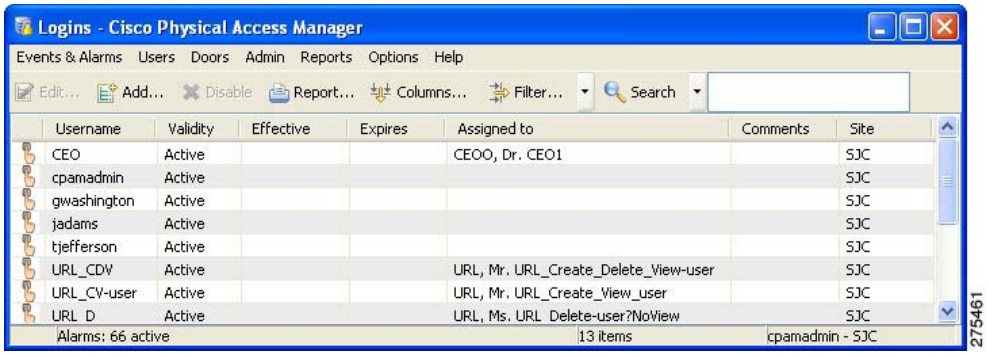
Step 10 Assign the profile to one or more Cisco PAM operators using the Logins module. (See the following section).

Creating User Login Accounts and Assigning Profiles

To give users access to Cisco PAM functionality, create a login account and assign one or more access profiles to the username.

Step 1 Select **Logins** from the Users menu. The main window (Figure 5-20) lists all the usernames in the system.

Figure 5-20 Logins Module Main Window



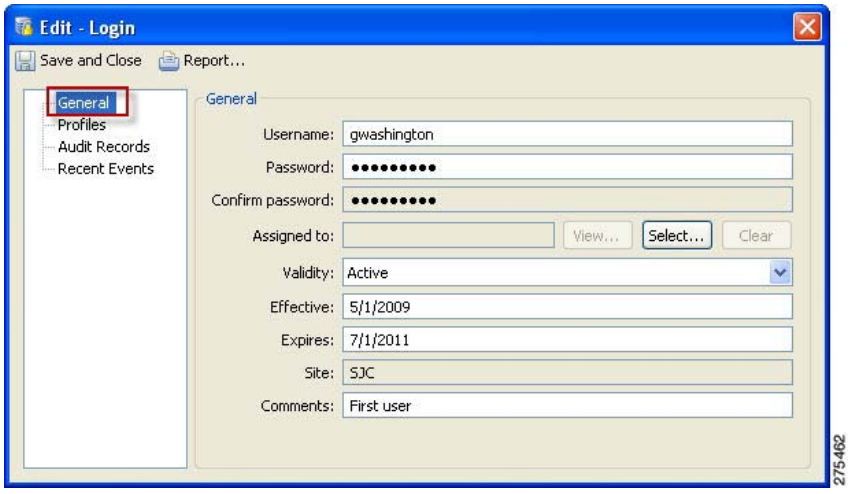
Step 2 To add a login, choose **Add**.

- To modify an existing login, select the entry and choose **Edit**.
- To remove a login, select the entry and choose **Delete**.

Note Most properties of the *cpamadmin* login are read-only.

Step 3 Complete fields in the General tab, as shown in Figure 5-21. Table 5-12 describes the field properties.

Figure 5-21 Logins Module—General Tab



Note The Username, Password, and Confirm password fields are required.

Table 5-12 General Tab Fields

Field	Description
Username	Required—The username of the login.
Password	Required—Password to access the system.
Confirm password	Required—The value must be entered exactly as it was in the Password field.
Assigned to	The personnel record the login is assigned to. If the login is for an operator already entered in the Personnel module, click the **Select...** button. For more information on adding personnel to the system, see Chapter 8, "Configuring Personnel and Badges" of the CPAM User guide.
Validity	Active or Inactive—Only active accounts can access the system.
Effective	The beginning date the user can log in—If left blank, the user can log in immediately.
Expires	The day the login expires and access is denied—If left blank, access is allowed indefinitely.
Site	Read-only—A site is a single instance of a Cisco PAM database.
Comments	Comments or notes about the login.

Step 4 Assign access privileges for the login:

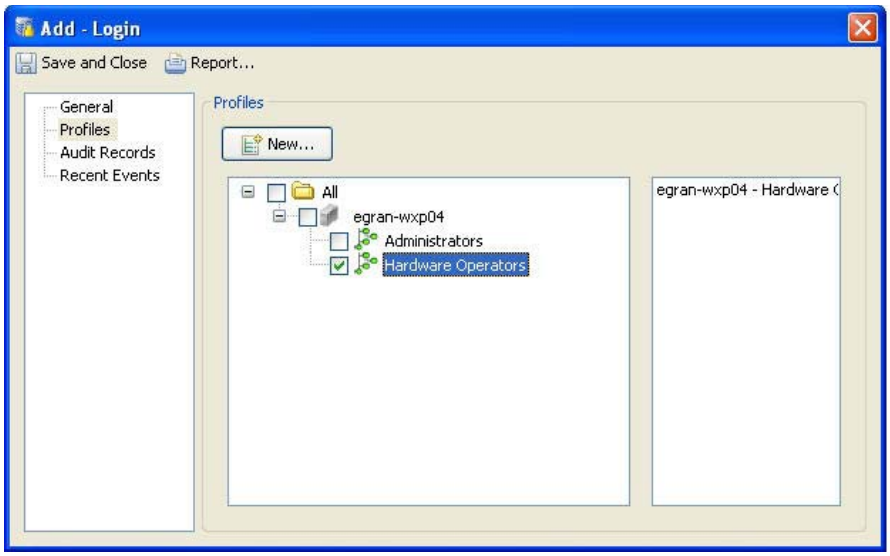
a. Select the **Profiles** tab, as shown in Figure 5-22.

b. Select the checkbox next to each profile to enable or disable access rights as defined by the access profile. For more information, see Defining User Profiles for Desktop Application Access.

c. Click **Save and Close** to save the changes and close the window.

Tip To create a new access profile, click the New button to open the Profiles module and refer to Defining User Profiles for Desktop Application Access.

Figure 5-22 Assigning One or More Profiles



Step 5 To verify the changes, log off and then log in with the new username and password. Verify that you can access the modules and functions specified by the assigned profiles.

- **PCI 7.2—***Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:*
  - **PCI 7.2.1—***Coverage of all system components*
  - **PCI 7.2.2—***Assignment of privileges to individuals based on job classification and function*
  - **PCI 7.2.3—***Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco PAM has a default policy of "Deny-all". If a specific badge has to get access to certain set of doors, an access policy must be created.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance with the sub-requirements in this section was achieved within the solution by implementing LDAP connectivity for AAA services and Microsoft Active Directory for user account services. Configure AAA services via LDAP, as shown in Requirement 8.2.

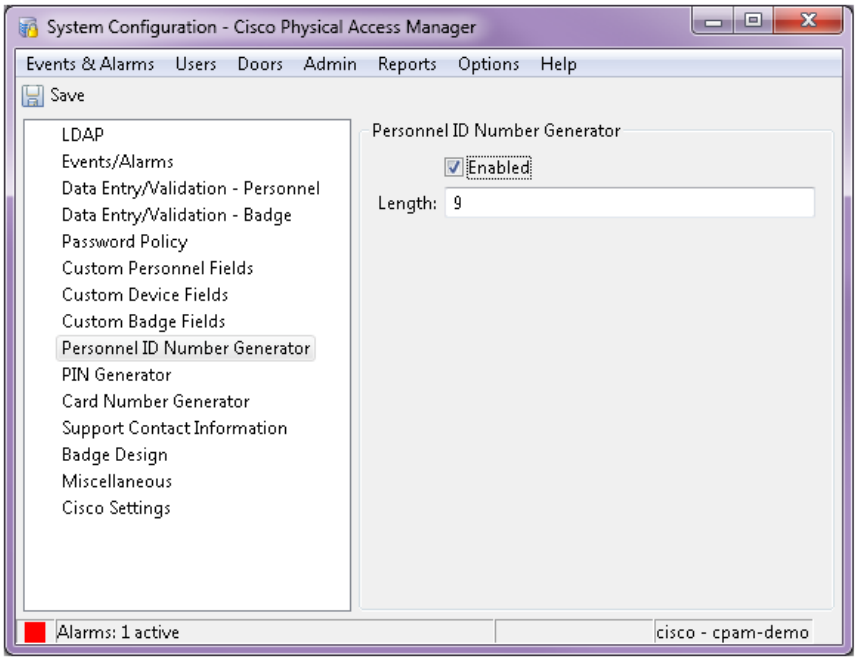
- **PCI 8.1—***Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco PAM integrates with Microsoft Active Directory (MS AD) to pull user information into CPAM. MS AD supports creation of unique ID for users. Cisco PAM has an option to generate a unique number for users using the Personnel ID Number Generator. It is disabled by default. Following are the instructions to enable and use this feature.

Step 1 On the Cisco PAM client application, open the System Configuration module by clicking **Admin -> System Configuration**.

Step 2 Click **Personnel ID Number Generator** on the left (see Figure 5-23) and check **Enabled**. Click **Save**.

Figure 5-23 Using the Personnel ID Number Generator

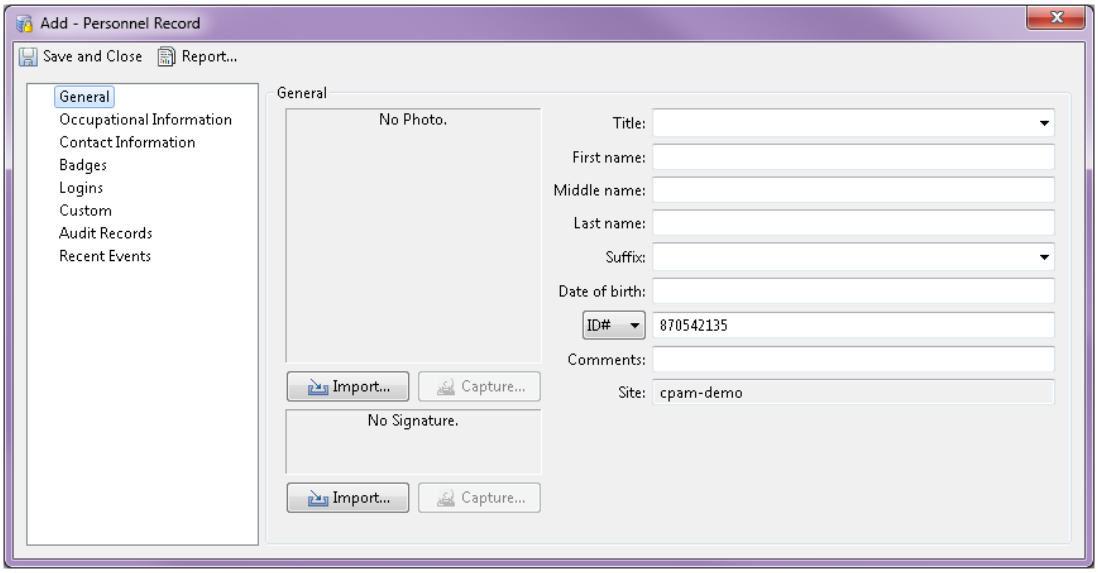


Step 3 Log out and log back into the Cisco PAM client to get the Personnel ID Number Generator featured working.

Step 4 Click on **Users -> Personnel**.

Step 5 Click **Add**. You should see a unique number generated automatically in the ID# field, as shown in Figure 5-24.

Figure 5-24 Unique ID Number



- **PCI 8.2—***In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Cisco PAM supports authentication through LDAP. Because LDAP supports this feature, Cisco supports the methods listed above.

Configuring LDAP User Authentication on Cisco PAM

To authenticate users using a Lightweight Directory Access Protocol (LDAP) server, do the following:

1. Configure the LDAP Server
2. Create the LDAP User Account in Cisco PAM

Configure the LDAP Server

Enter the LDAP server settings to configure the LDAP server connection and user authentication, as described in the following steps.

Step 1 Select **System Configuration** from the Admin menu, and then select the **LDAP** tab.

Step 2 Enter the LDAP user authentication settings. The LDAP configuration depends on the authentication mode:

- User principal name (recommended method)—The user principal name is unique in the organization.
- sAMAccountName—The sAMAccount username is unique only in the search domain.

LDAP uses a principle to authenticate. The principle is formed from the username: prefix + username + suffix. The exact format of the principle varies based on the type of LDAP server, and the domain.

For OpenLDAP, the prefix should be: uid=
The suffix should be changed to reflect the actual domain.
So for my-domain.com, this would be:
,dc=my-domain, dc=com

For more information, see the following:

- LDAP Example: User Principal Name
- LDAP Example: sAMAccountName

Step 3 Enter the other LDAP server settings, as listed in Table 5-13.

Table 5-13 LDAP System Configuration Settings

Field	Description
Enable LDAP	Click the checkbox to enable or disable LDAP support.
LDAP server URL	URL of LDAP server, must begin with ldap:// Example: ldap://192.168.1.1:389 **Note** 389 is the port number.
Principle suffix	Appended to the username for authentication. See above.

Table 5-13 LDAP System Configuration Settings (continued)

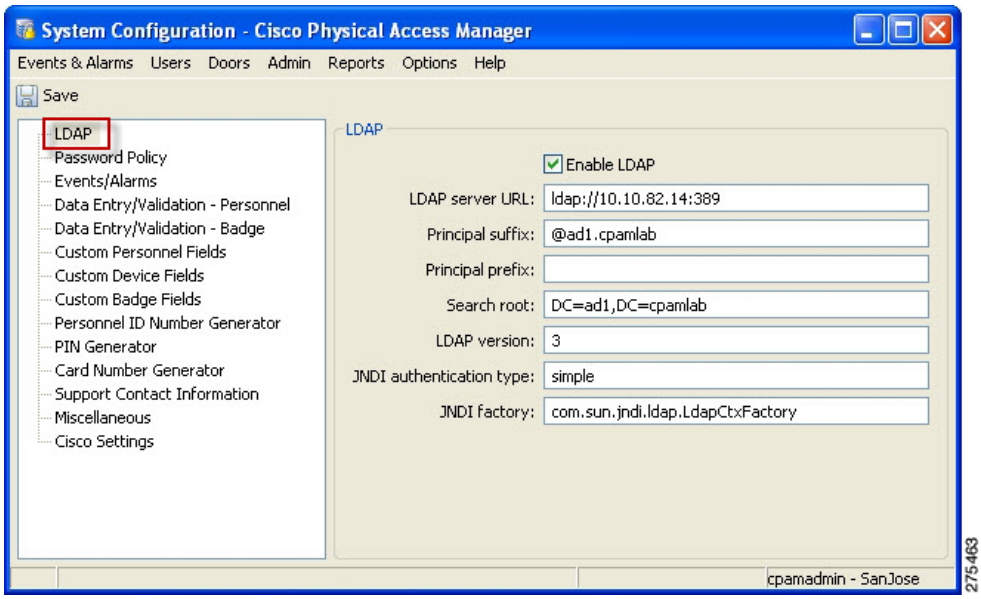
Principle prefix	Prepended to the username for authentication. See above.
Search root	LDAP search root. The search root is the node in the LDAP tree, the subtree under which the user account should be found. • For Active Directory, the dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com: cn=Users, dc=my-domain, dc=com. • For OpenLDAP, the 2 dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com:dc=my-domain,dc=com.
LDAP version	An advanced setting that generally should be left unchanged.
JNDI authentication type	An advanced setting that generally should be left unchanged as simple.
JNDI factory	An advanced setting that generally should be left unchanged as com.sun.jndi.ldap.LdapCtxFactory

Step 4 Log out and log back in to the Cisco PAM application to enable the changes (select **Logout** from the Options menu).

LDAP Example—User Principal Name

In the example shown in Figure 5-25, the user principal name is *cpsm.user@ad1.cpamlab*. The Cisco PAM user login must be the same (*cpsm.user*).

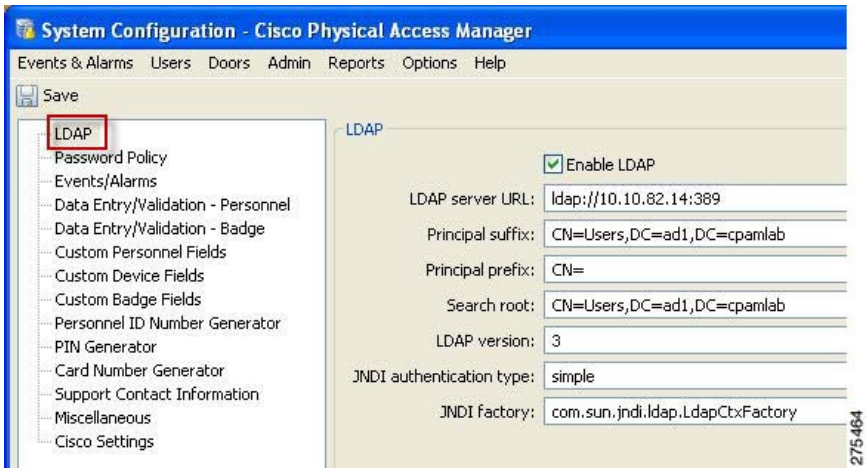
Figure 5-25 User Principal LDAP Configuration Example



LDAP Example—sAMAccountName

In the example shown in Figure 5-26, the user login is the same as the samaccount name (*cpsmuser*).

Figure 5-26 sAMAccountName—LDAP Configuration Example

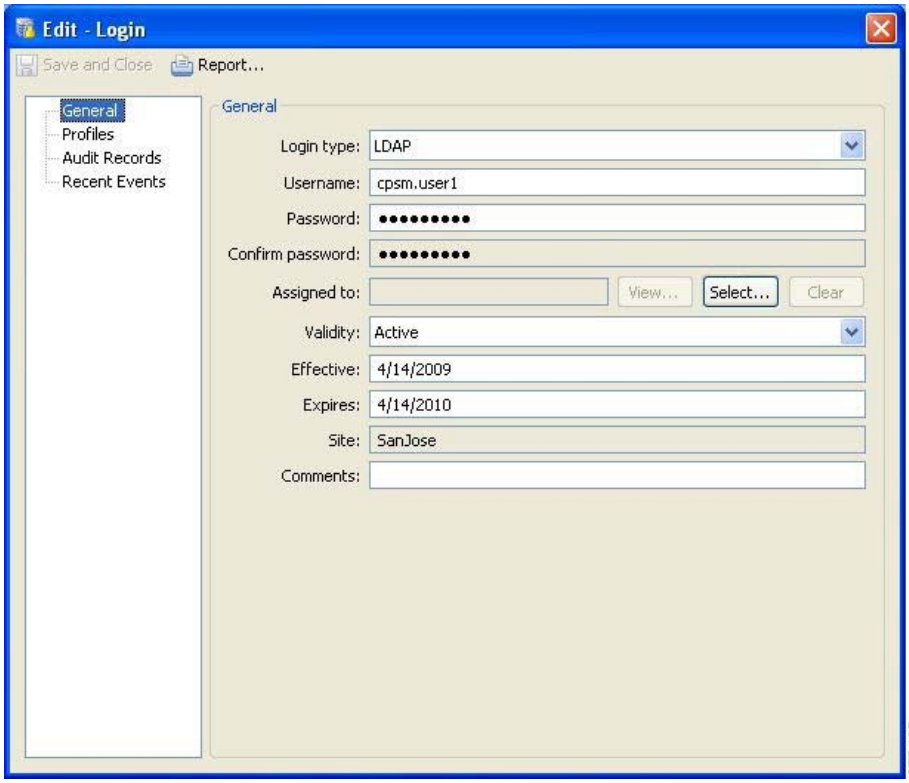


Creating the LDAP User Account in Cisco PAM

Create the user account to be authenticated using an LDAP server with the following steps.

Step 1 Select **Logins** from the Users menu. (See Figure 5-27.)

Figure 5-27 Login Window: LDAP Login Type



Step 2 Click **Add**, or select an existing login and click **Edit**.

Step 3 Select the Login type **LDAP**. The Login type field appears only if LDAP was enabled and the Cisco PAM application was restarted (see Configure the LDAP Server).

Step 4 Enter the username, password, and other settings for the LDAP login. See Creating User Login Accounts and Assigning Profiles.

Note Although a password must be entered for all user Login records, it is not used for LDAP authentication. LDAP servers use the password entered when the user logs in to Cisco PAM.

Step 5 Click **Profiles** and select the user's Cisco PAM profiles. See Defining User Profiles for Desktop Application Access for more information.

Note Cisco PAM does not synchronize the LDAP profiles.

Step 6 Click **Save and Close**.

The following requirements (8.4, 8.5.5, 8.5.9–14) are all met through the use of LDAP as the authentication services:

- **PCI 8.4—***Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5—***Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9—***Change user passwords at least every 90 days.*
- **PCI 8.5.10—***Require a minimum password length of at least seven characters.*
- **PCI 8.5.11—***Use passwords containing both numeric and alphabetic characters.PCI Sub-Requirements with Compensating Controls*
- **PCI 8.5.12—***Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13—***Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14—***Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15—***If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco PAM has a hard-coded session timeout of 30 minutes in the configuration for the version validated. Administration time limits would need to be enabled systemically through an active directory policy to the admin workstation desktops, locking them when there is no activity after 15 minutes.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco PAM is able to track and monitor all administrative user access and events to meet the following requirements**:**

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*

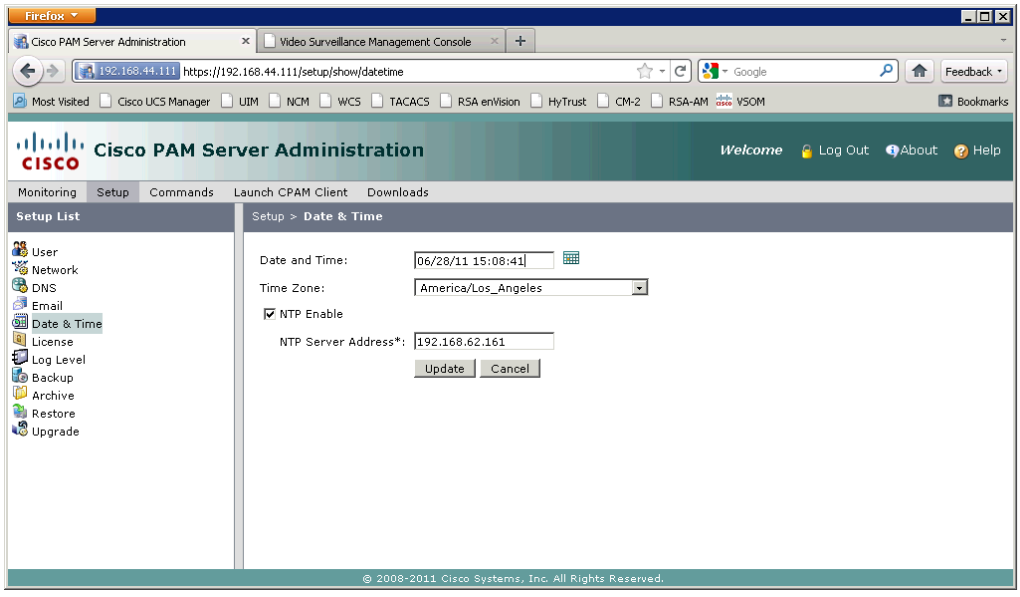
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco PAM and the gateways use the local clock facilities to meet the following requirements**:**

- **PCI 10.4.2—***Time data is protected.*
- **PCI 10.4.3—***Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. All the events in the Access Control system have a time stamp associated to them. Cisco PAM and the gateway are configured to use NTP, as shown in Figure 5-28.

Figure 5-28 Cisco PAM NTP Configuration



Requirement 10.5 was met using a central logging repository, RSA enVision, which collects logging information from all devices to ensure the integrity and correlation of events.

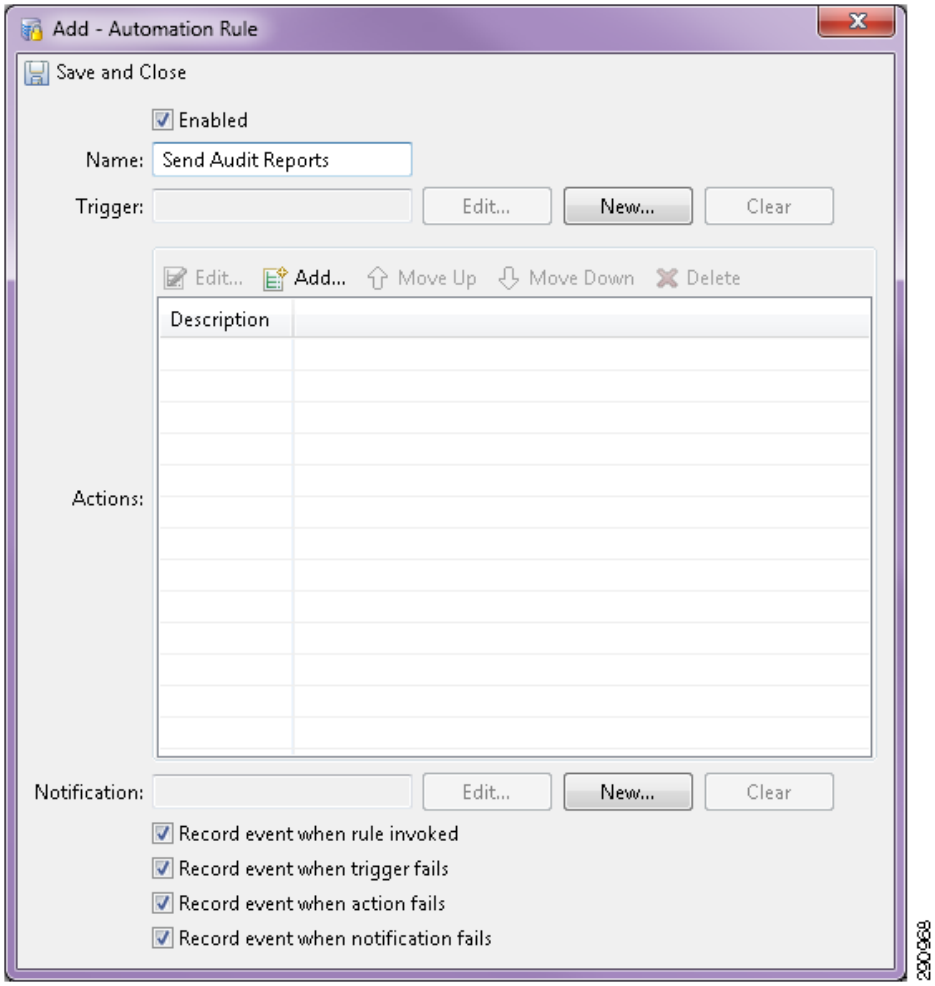
- **PCI 10.5—***Secure audit trails so they cannot be altered.*
- **PCI 10.5.1—***Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2—***Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3—***Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5—***Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco PAM allows for the creation of global I/O rules to trigger sending audit reports to a centralized server. Following are the instructions to create a global I/O with audit reports.

Step 1 In the Cisco PAM client, click **Events & Alarms -> Global I/O > Add**.

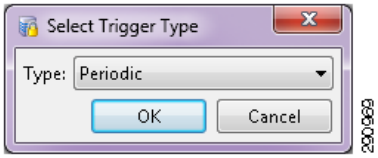
Step 2 Enter a name and click **New** in the Trigger field. (See Figure 5-29.)

Figure 5-29 Creating a Global I/O with Audit Reports



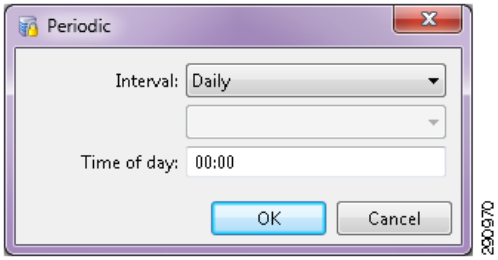
Step 3 Select **Periodic** and click **OK**. (See Figure 5-30.)

Figure 5-30 Selecting Periodic



Step 4 Choose the Interval and enter the Time of Day. Click **OK**. (See Figure 5-31.)

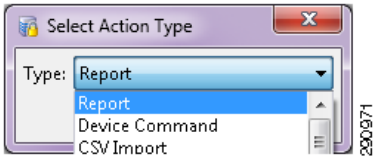
Figure 5-31 Selecting Interval and Time of Day



Step 5 Under Actions, Click **Add…**

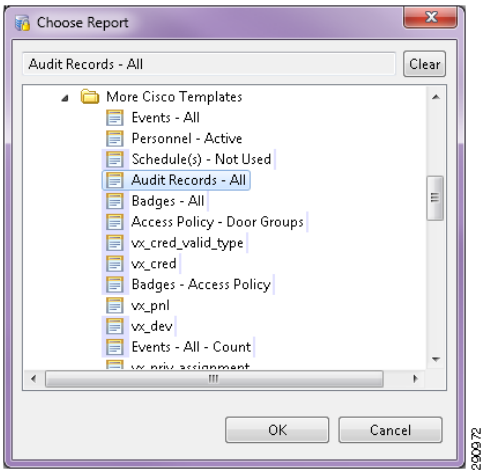
Step 6 Select **Report.** (See Figure 5-32.)

Figure 5-32 Selecting Action Type



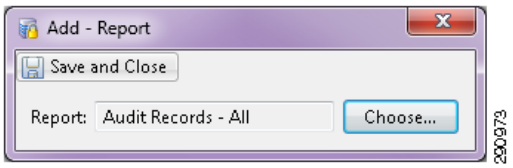
Step 7 Choose **Audit Records–All** and click **OK**. (See Figure 5-33.)

Figure 5-33 Audit Records–All



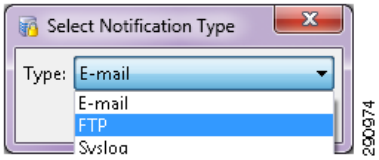
Step 8 Click **Save and Close**. (See Figure 5-34.)

Figure 5-34 Save and Close



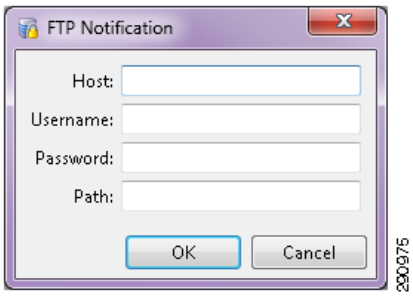
Step 9 Under Notification section of the Global I/O, click **New** and Choose **FTP**. Click **OK**. (See Figure 5-35.)

Figure 5-35 Select Notification Type



Step 10 Enter the FTP Host, Username, Password, and Path. Click **OK**. (See Figure 5-36.)

Figure 5-36 FTP Notification



Step 11 Click **Save and Close**. You should see a new entry created. You can create similar global I/O rules for every hour.

The audit report is read into RSA enVision server, which then maintains and protects the integrity of the file.

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

E-mail

Cisco IronPort Email Security Solution

Cisco IronPort Email Security Solution uses data loss prevention (DLP) technology to block e-mail that is inadvertently sent containing cardholder data information.

Note The Cisco IronPort Email Security Solution was initially reviewed by Verizon Business and determined to be outside the scope of the PCI Audit. There is no Assessment Summary or Capability Assessment details for this product. However, Cisco IronPort Email Security Solution could potentially store or transmit sensitive cardholder data if used with the default settings for message tracking. Sensitive information in messages would be automatically forwarded in clear text to administrators, and recipients. These same messages would also be stored un-encrypted. The design considerations below detail how to properly configure the Cisco IronPort Email Security Solution to avoid this pitfall.

Cisco IronPort Email Security Solution provides sophisticated and scalable mechanisms that help to minimize the downtime associated with e-mail-borne malware and simplify the administration of corporate e-mail systems, while offering insight into the e-mail system operation. Capabilities include the following:

- Spam protection
- Data loss prevention (DLP)
- Virus defense
- E-mail encryption tracking and reporting tools

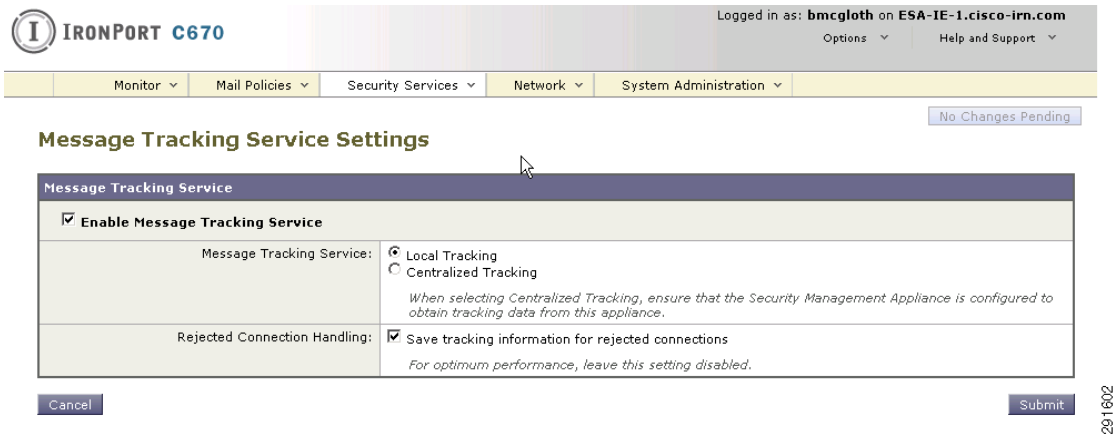
Primary PCI Function

Although data loss prevention is not covered by a specific PCI requirement, Cisco IronPort Email Security Solution helps in achieving PCI compliance by preventing the transmission of cardholder data over open public networks via e-mail.

Design Considerations

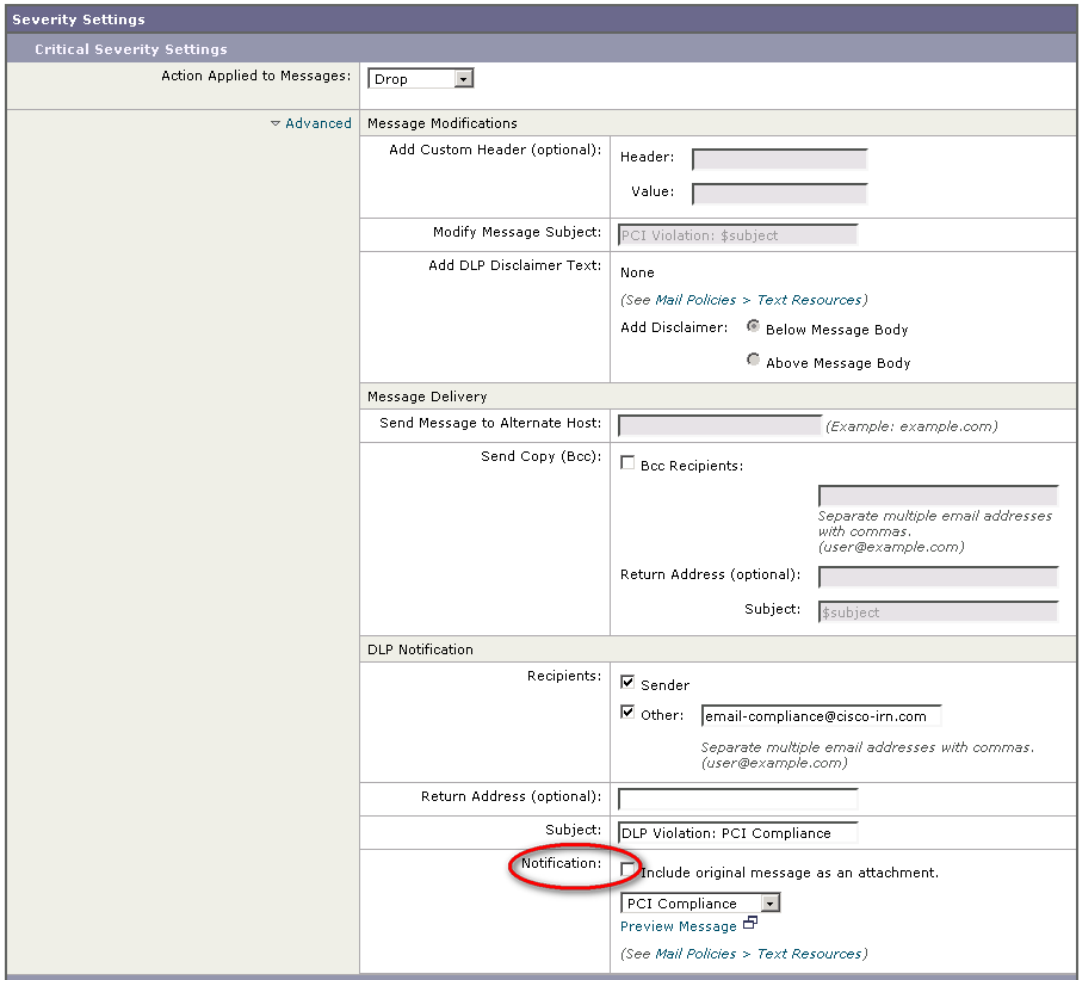
- Do not enable logging, storage, or forwarding messages identified as containing cardholder data.
- For IronPort to analyze messages passing through it, message tracking must be enabled, as shown in Figure 5-37.

Figure 5-37 Enable IronPort Message Tracking



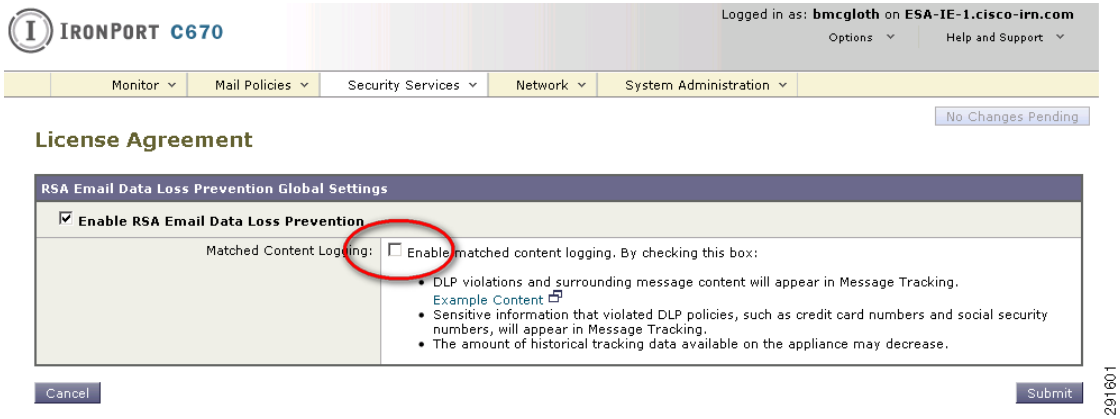
- Create policy in IronPort to drop messages containing credit card numbers, but not to forward that message to administrators. Ensure that the "include original message" checkbox is not selected, as shown in Figure 5-38.

Figure 5-38 Policy in IronPort Excluding Original Message



- To ensure that messages identified as containing credit card information are not stored in the local system, you must disable logging of matched content, as shown in Figure 5-39. The local log of the IronPort server is not a safe encrypted place to store cardholder data.

Figure 5-39 IronPort DLP—Matched Content Logging Disabled



Hosts

Cisco Unified Computing System

The Cisco Unified Computing System (UCS) is used to securely deploy sensitive and compliance-related applications. Provisioning options, including virtualization technology, allow the mixing of sensitive and non-sensitive applications without compromising scope boundaries.

Improve IT responsiveness to rapidly changing business demands with this next-generation data center platform. Cisco UCS accelerates the delivery of new services simply, reliably, and securely through end-to-end provisioning and migration support.

Benefits include the following:

- Streamlines data center resources to reduce total cost of ownership
- Scales service delivery to increase business agility
- Radically reduces the number of devices requiring setup, management, power, cooling, and cabling

Table 5-14 PCI Assessment Summary—Cisco UCS

Models Assessed	
Cisco UCS Manager version 1.3(1p)	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15

Table 5-14 PCI Assessment Summary—Cisco UCS (continued)

PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

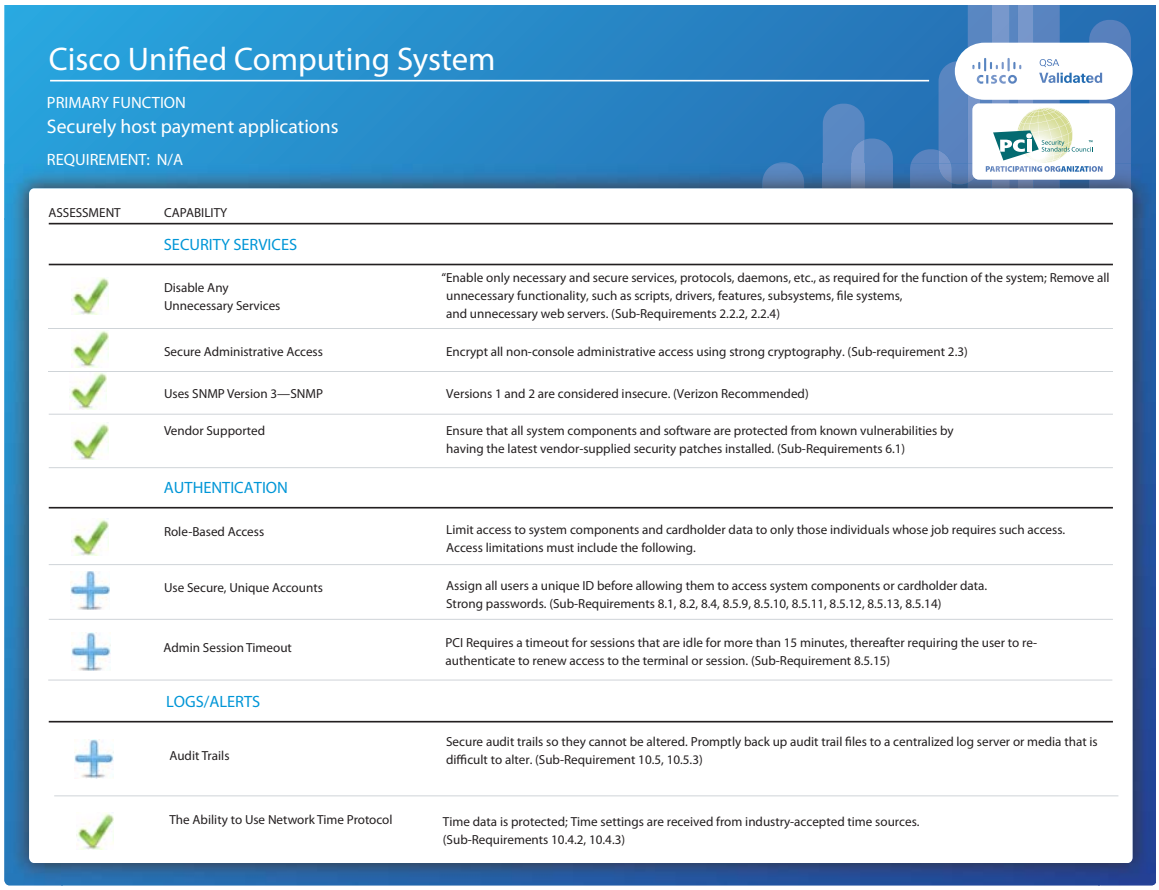
Primary PCI Function

The main function of Cisco UCS is to securely host one primary compliance-related function per physical or virtual server.

It provides segmentation of sensitive applications from out-of-scope applications via physical and virtualization technology. Although technically, a firewall or ACL is used to enforce PCI Requirement 1, Cisco UCS extends Layer 3 boundaries to virtual network and storage adapters within the chassis. Using VLANs and VSANs, Cisco UCS allows an organization to separate its payment systems (in-scope) from other non-sensitive data (out-of-scope).

Table 5-15 lists the component assessment details for Cisco UCS.

Table 5-15 Component Capability Assessment—Cisco Unified Computing System



Cisco Unified Computing System

PRIMARY FUNCTION
Securely host payment applications
REQUIREMENT: N/A

cisco QSA Validated

PCI Security Standards Council PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
✓	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Cisco UCS allows for the provisioning of individual servers on blades. Each blade can host a native operating system such as Windows 2008 server, or a virtualization hypervisor system such as VMware ESX/ESXi. These provisioning options represent a primary function for the server blade. In the lab validation, VMware ESX was installed on each of the Cisco UCS blades, and several VM hosts were then configured, each with one primary function. Each server blade is provisioned via a profile. Profiles can be created locally in Cisco UCS Manager or centrally using the Vblock provisioning utility, Unified Infrastructure Manager (UIM), which provides simplified Vblock management by combining provisioning with configuration, change, and compliance management.
- EMC SAN is a primary component of the VCE architecture for Vblock Infrastructure Platforms. Vblock 1 is designed for medium to high numbers of virtual machines, and is ideally suited to a broad range of usage scenarios, including shared services, e-mail, file and print, virtual desktops, and collaboration.
- Cisco UCS allows for the provisioning of individual servers on blades. Each blade can host a native operating system such as Windows 2008 server, or a virtualization hypervisor system such as VMware ESX/ESXi.
- Each Cisco UCS server blade is provisioned via a profile. Profiles can be created locally in Cisco UCS Manager or centrally using the Vblock provisioning utility, EMC Unified Infrastructure Manager (UIM), which provides simplified Vblock management by combining provisioning with configuration, change, and compliance management.
- The PCI standard requires one primary function per server. When using virtualization technology, the single primary server function is extended to individual virtual machines.
- The hypervisor of an individual blade is considered insecure for segmenting scopes of compliance. Therefore, when putting non-sensitive VM servers with sensitive VM servers on the same physical blade, the non-sensitive would be included in the scope of the audit.
- The UCS system securely segments network and storage to each blade, which allows mixing of sensitive and non-sensitive applications across different physical blades of the chassis.
- PCI requires a 15-minute timeout for administrative functions. Cisco UCS does not feature an explicit session timeout. Administration time limits would need to be enabled systemically through active directory policy to the admin workstation desktops, locking them when there is no activity.

  Cisco UCS was implemented using the Cisco UCS installation guides: http://www.cisco.com/en/US/products/ps10276/prod_installation_guides_list.html

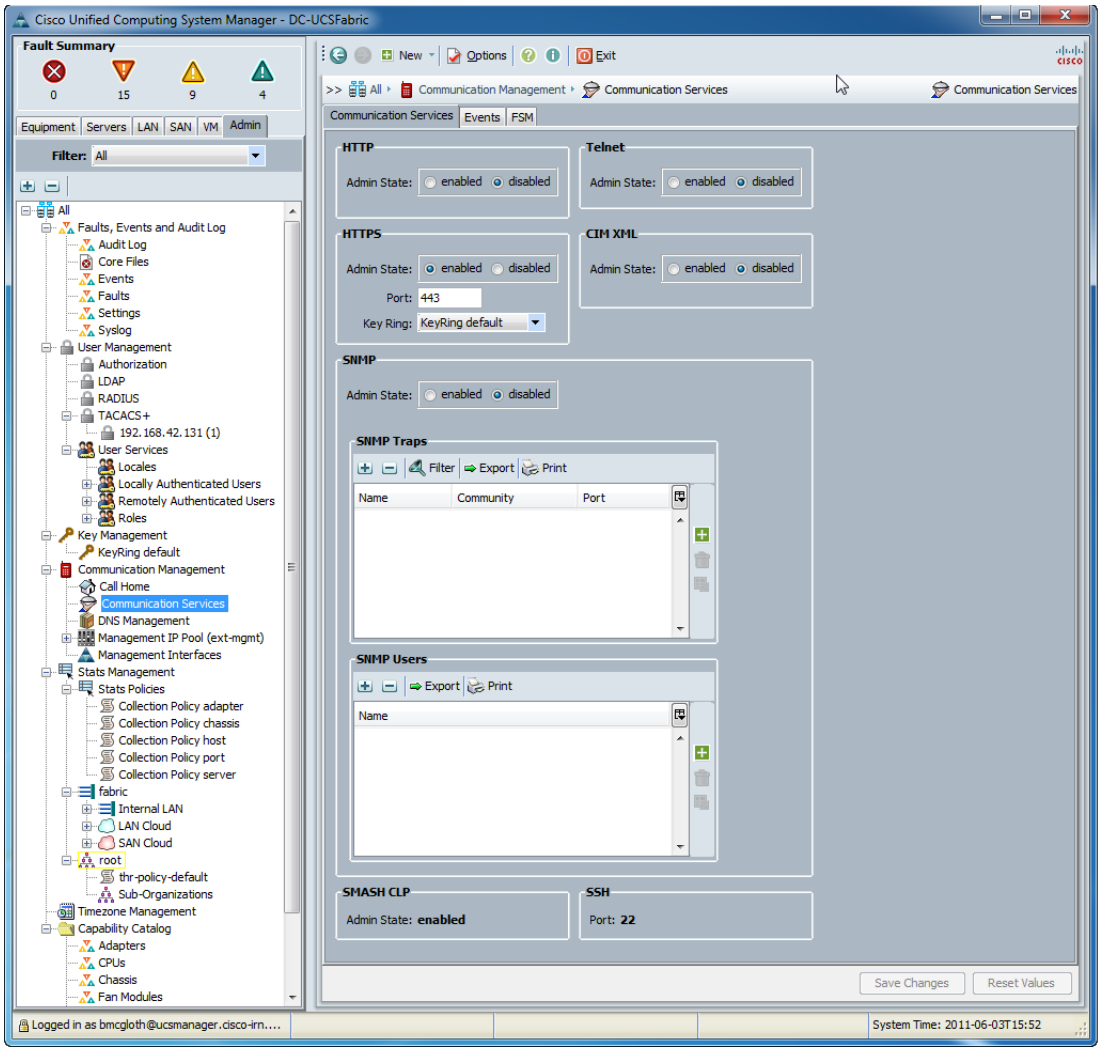
PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco UCS allows for the disabling of non-secure administrative interfaces. Figure 5-40 shows the secure management protocols of SSH and HTTPS for administration. Telnet, HTTP, and other unused protocols are disabled.

Figure 5-40 Secure Management Protocols



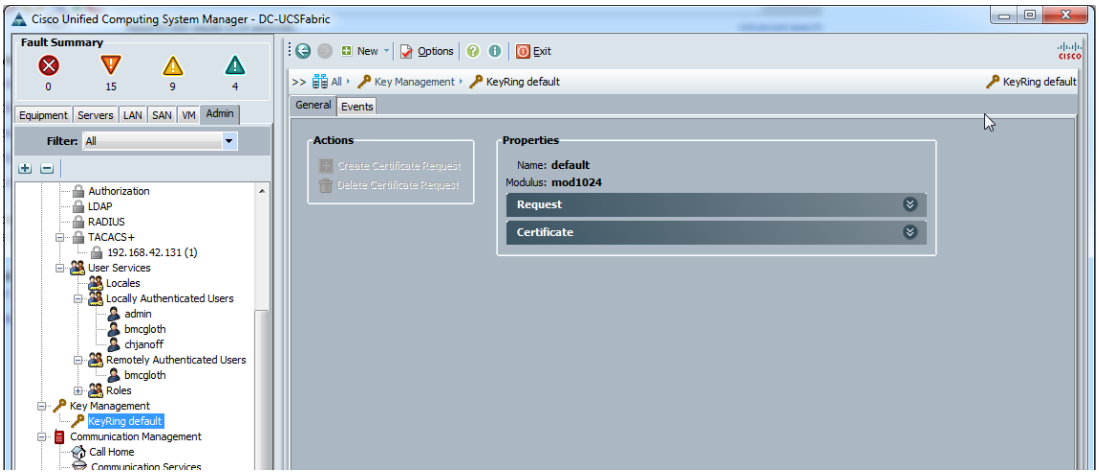
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco UCS does not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco UCS uses strong encryption for SSH and HTTPS connections. Encryption keys are created and managed under the Key Management feature. (See Figure 5-41.)

Figure 5-41 1024-Bit Mod Key Default Keyring



Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco UCS. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

  For more information about PSIRT, see the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

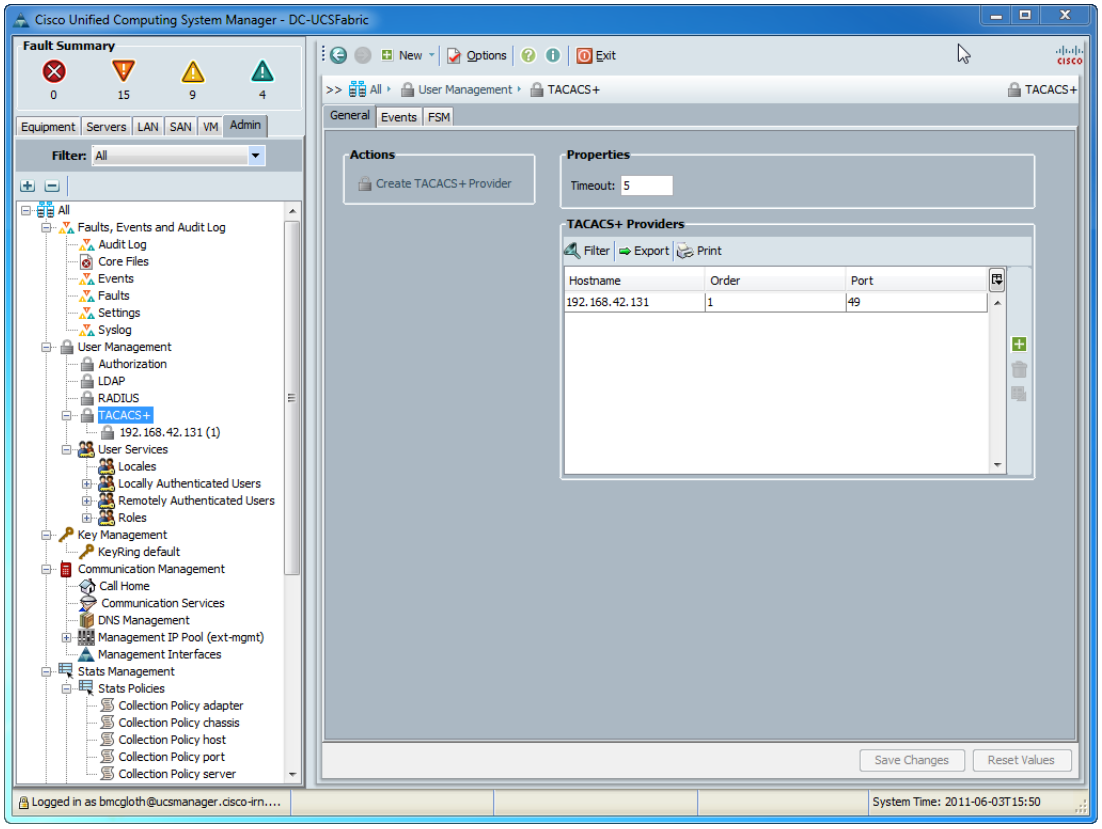
The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

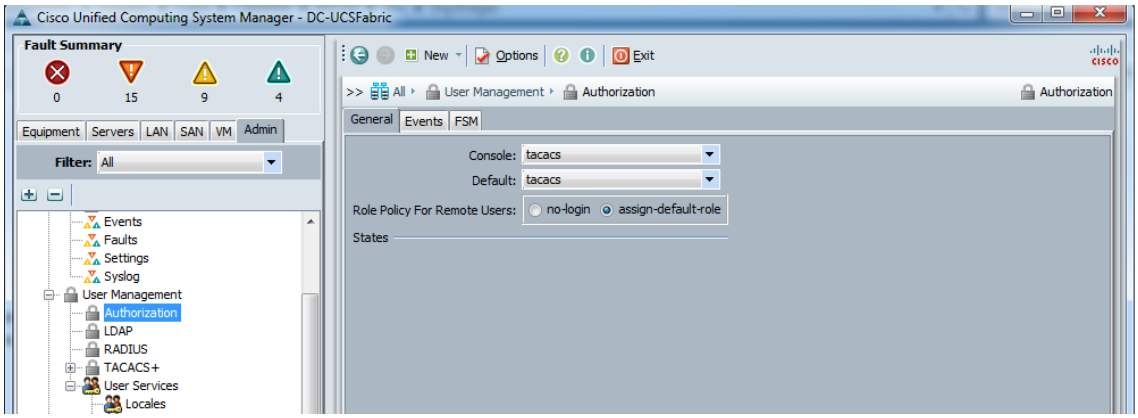
Add the Cisco Secure ACS server under the TACACS+ protocol option, as shown in Figure 5-42.

Figure 5-42 Adding the Cisco Secure ACS Server



Select **tacacs** from the Console and Default dropdown menus on the Authorization page, as shown in Figure 5-43.

Figure 5-43 Authorization—Selecting Console and Default Settings



On the TACACS+ server, create custom attributes defining the desired role for the user or group accessing the Cisco UCS Manager (see Figure 5-44):

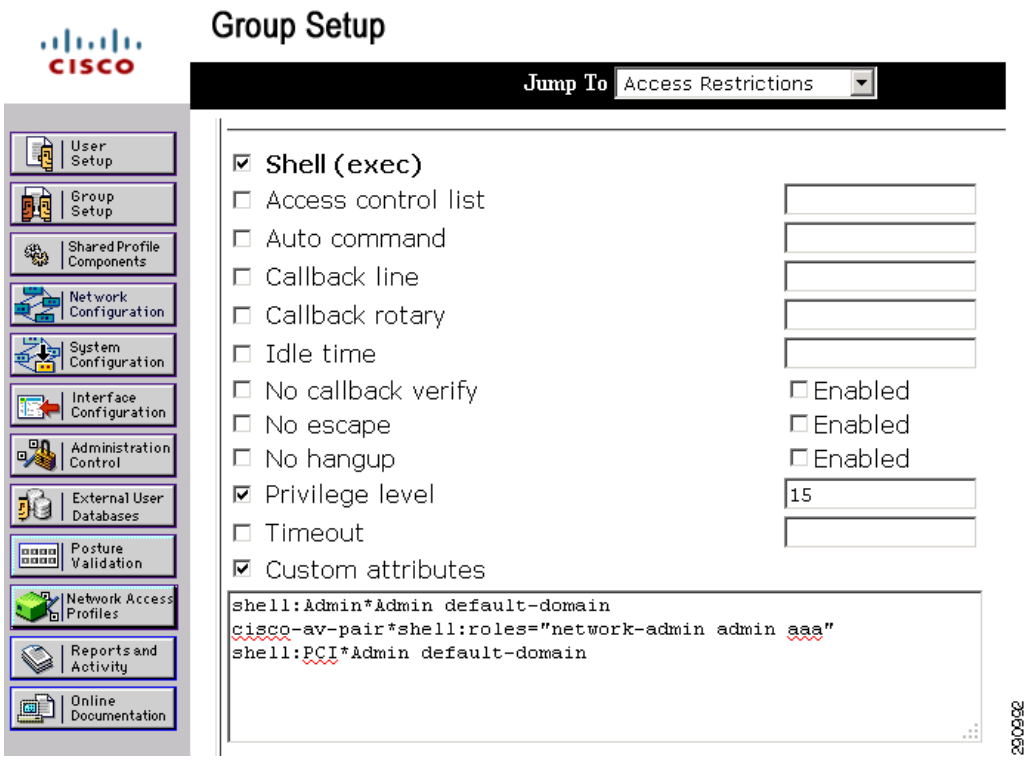
- TACACS+ custom attributes for UCS Manager:

```
cisco-av-pair*shell:roles="admin aaa"
```

- If combined with other systems roles, such as for the Nexus;

```
cisco-av-pair*shell:roles="network-admin admin aaa"
```

Figure 5-44 Group Configuration Page on TACACS+ Server



Requirement 8: Assign a Unique ID to Each Person with Computer Access

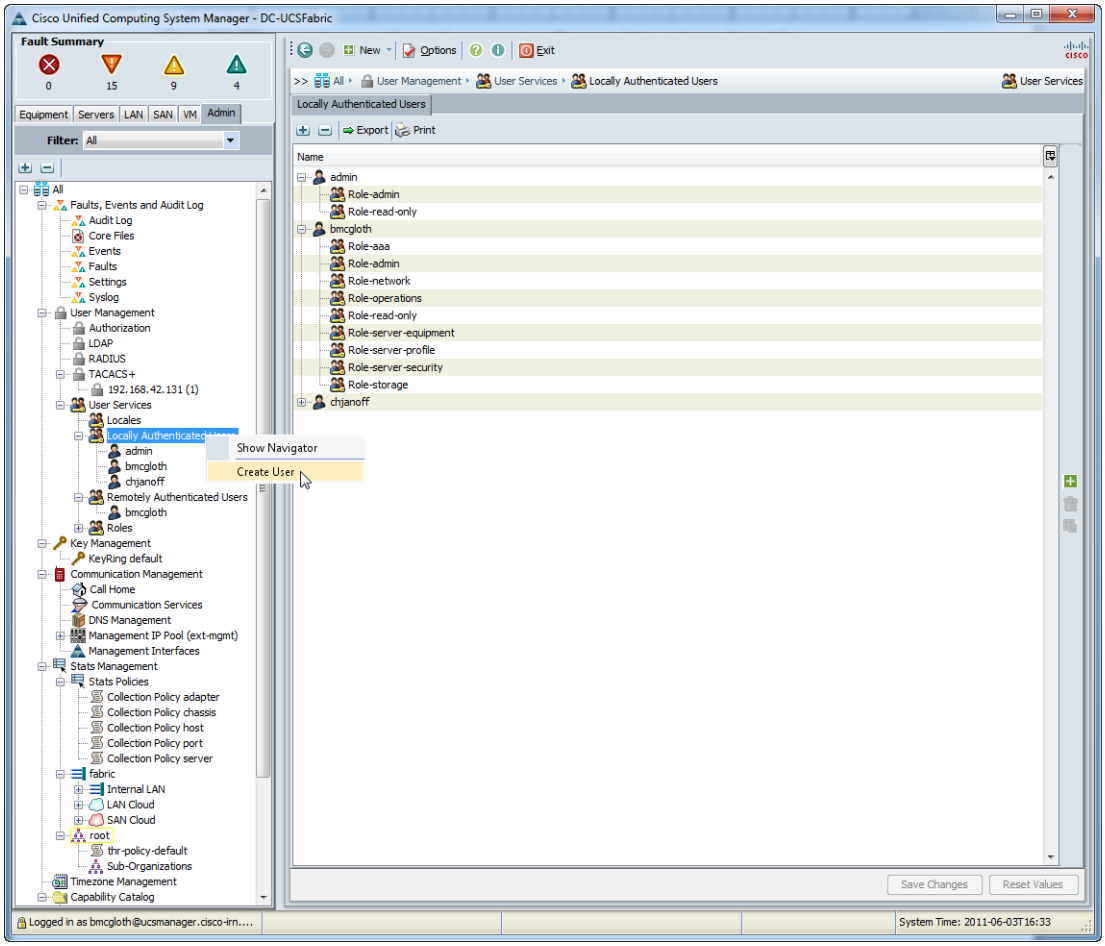
Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown above in Requirement 7.

The Cisco UCS is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco UCS supports the creation of local user accounts with unique IDs through the use of the Create User option when you alt-click on Locally Authenticated Users (see Figure 5-45). These can be used for local fallback user accounts.

Figure 5-45 Create User



- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco UCS require setting of a password for admin role accounts.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Local passwords are stored encrypted on the Cisco UCS system and are not displayed.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco UCS servers allow for an administrator to specify an expiration date for the local user accounts passwords, effectively disabling their accounts after a specified period of time.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco UCS does not support an automated capability to perform this function at this time; user passwords management would have to be manually performed every 90 days per a company policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco UCS servers require a minimum of eight characters for local passwords.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters. PCI Sub-Requirements with Compensating Controls*

  Cisco UCS servers require at least three of the following character types for passwords:

  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco UCS does not support an automated capability to perform this function at this time; user account management would have to follow this policy manually if a centralized authentication service with this capability could not be used.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco UCS does not support the ability to lock out local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco UCS does not support the ability to lock out local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco UCS does not feature an explicit session timeout. Administration time limits would need to be enabled systemically through an Active Directory policy to the admin workstation desktops, locking them when there is no activity after 15 minutes.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco UCS is able to track and monitor all administrative user access, events such as profile creation, interface up/down, and device authentications.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco UCS is able to track and monitor all administrative user access and events.

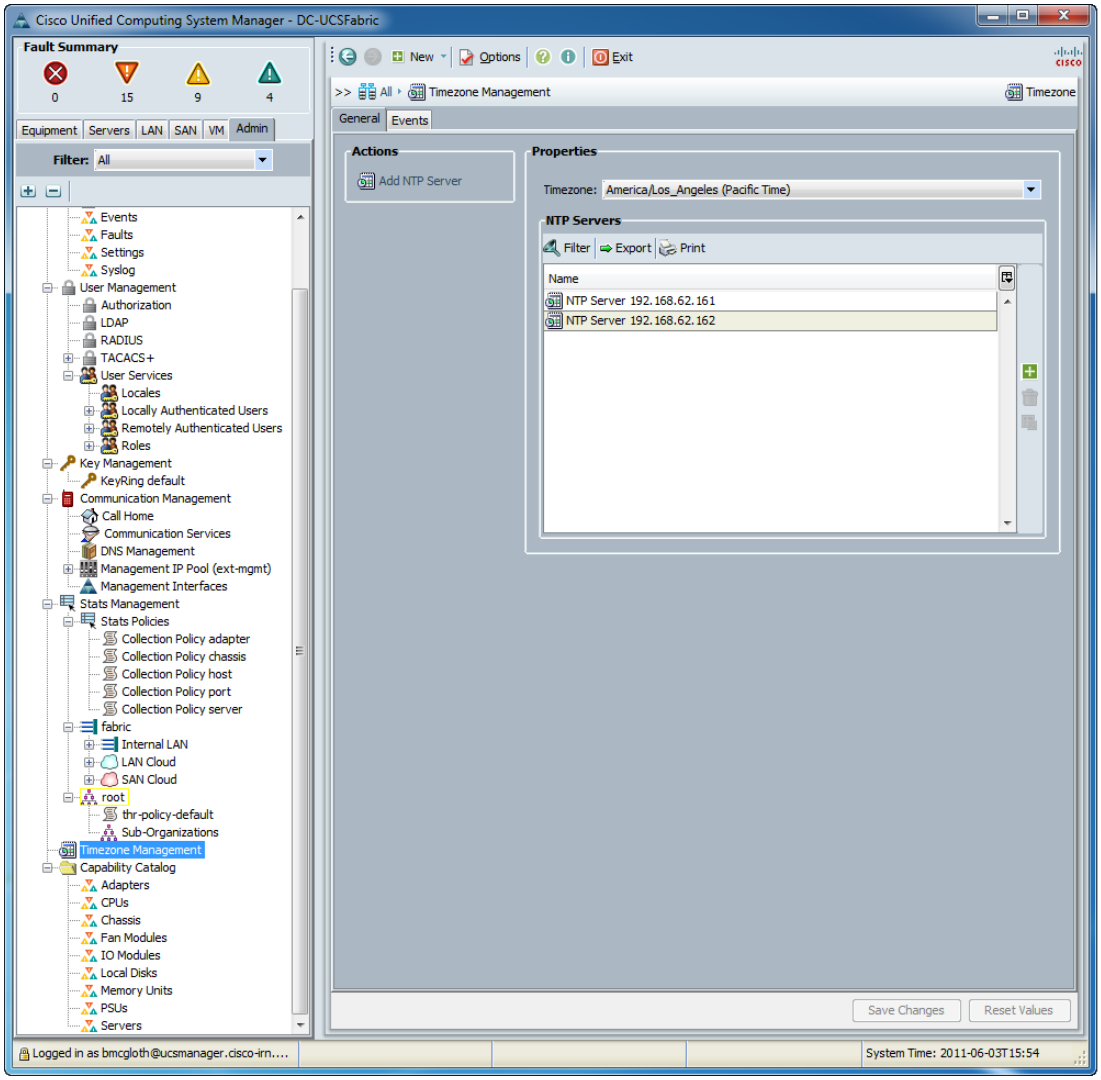
- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco UCS uses NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices (see Figure 5-46). This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

Figure 5-46 NTP Screen



To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

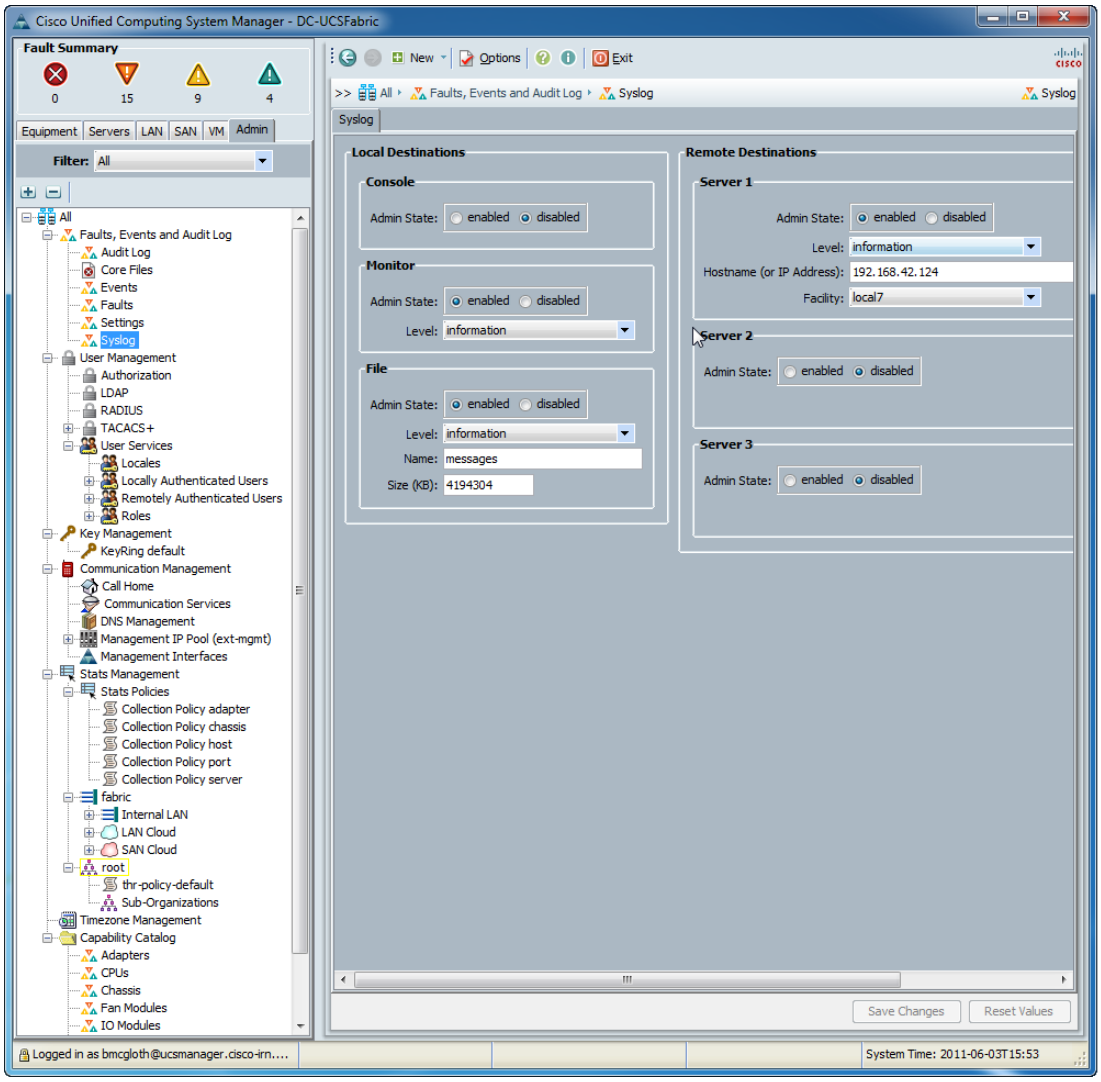
Requirement 10.5 was met using RSA enVision, which is a central logging repository that collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*

- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco UCS is capable of sending system events to a centralized repository using the syslog function and/or SNMP traps. In the solution, only syslog was used. (See Figure 5-47.)

Figure 5-47 Using Syslog



PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco UCS Express on Services Ready Engine

The Cisco Unified Computing System (UCS) Express and Services Ready Engine (SRE) allows organizations to securely deploy sensitive applications directly within the routing platform. By usingthe UCS E-series, organizations can remove legacy compute resources in the branch, saving space, energy, and operational costs.

Cisco UCS E-series is a converged networking, computing, and virtualization platform for hosting essential business applications in the branch location. The SRE modules are router blades for the second generation of Cisco Integrated Services Routers (ISR G2) that provide the capability to host Cisco, third-party, and custom applications. A service-ready deployment model enables branch applications to be provisioned remotely on the modules at any time. Cisco SRE modules have their own processors, storage, network interfaces, and memory, which operate independently of the host router resources and help ensure maximum concurrent routing and application performance.

Table 5-16 PCI Assessment Summary—Cisco UCS Express and Cisco SRE

Models Assessed	
Cisco UCS Express version 1.1 on SRE900	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.15, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No sub-requirements were failed.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of the Cisco UCS Express is to securely host one primary compliance-related function per physical or virtual server.

It provides segmentation of sensitive applications from out-of-scope applications via physical and virtualization technology. Although technically, a firewall or ACL is used to enforce PCI Requirement 1, UCS extends Layer 3 boundaries to virtual NIC and storage adapters within the chassis. Using VLANs and VSANs, Cisco UCS allows an organization to separate its payment systems (in-scope) from other non-sensitive data (out-of-scope).

Table 5-17 lists the component assessment details for the Cisco UCS Express and Cisco SRE.

Table 5-17 Component Capability Assessment—Cisco UCS Express and Cisco SRE

Cisco UCS Express and Cisco SRE

PRIMARY FUNCTION
Securely host payment applications

REQUIREMENT: N/A

QSA Validated

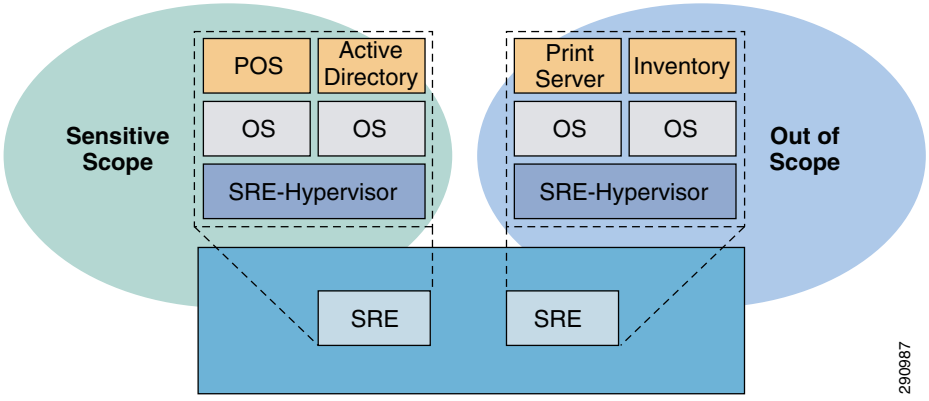
PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

The major consideration when using Cisco UCS Expresss with sensitive applications is the security of the hypervisor. PCI considers all hypervisors to be insecure. Therefore, use separate Cisco UCS Express implementations when scooping. Although it is acceptable to mix non-sensitive applications onto a Cisco UCS Express deployment with sensitive applications, that brings those applications into scope and audit. (See Figure 5-48.)

Figure 5-48 Using UCS Express with Cisco SRE



- The audited version 1.5 of UCS Express has several limitations with local user accounts. There is no capability to use central authentication or management. This resulted in a need for compensating controls that are detailed below.

Note Newer versions of UCS Express (version 1.5 +) enable central management of the VMware ESXi on Cisco UCS Express through vCenter (upgrade license required) as well as eliminate the Cisco console VM and local user management/VMware ESXi management restrictions. With the new release, Cisco UCS can manage users on VMware ESXi exactly as it would on a standalone VMware ESXi 4.1 server.

Note The Cisco UCS Express module comes installed with VMware ESXi. This is the primary function for the server module. Each module can host several independent operating systems as virtual servers. Each virtual server should have only one primary function.

- Cisco UCS Express requires the use of VLANs in the router. Depending on the deployment within the branch, this may require the use of bridged virtual interfaces.
- Cisco UCS Express is based on VMware's ESXi and uses vSphere client for management.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco UCS Express and the underlying VMware ESXi have no unnecessary services enabled by default.
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco UCS Express appliance does not allow changes to the operating system, installation of unsupported hardware, or of unsupported third-party software.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco UCS Express uses strong encryption for SSH and HTTPS connections.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco UCS Express. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html.

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT, see the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the vCenter database for administrator users. Individual administrative user IDs are created and assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco UCS Express includes extensive controls for defining user privileges and by default denies access to all individuals without a system user ID.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of the ESX hypervisor as part of the vSphere and vCenter infrastructure.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco UCS Express supports the creation of local user accounts with unique IDs through the use of the VMware vSphere client editing the local users and groups database.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco UCS Express require setting of a password.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

All passwords are stored using strong encryption.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Administrative time limits would need to be enabled systemically through an active directory policy to the admin workstation desktops, locking them when there is no activity.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  PCI 8.5.14—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco UCS Express is able to track and monitor all administrative user access, events such as profile creation, interface up/down, and device authentications.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

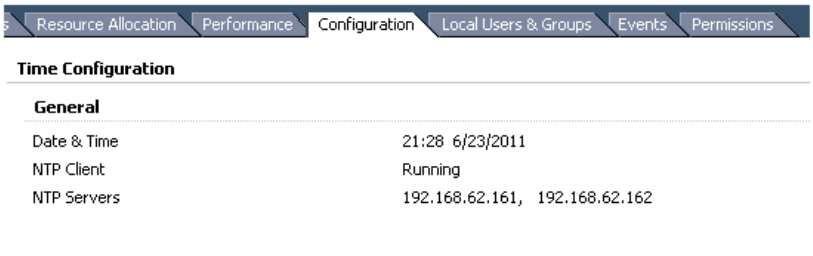
Cisco UCS Express uses the local clock facilities to meet the following requirements:

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*

- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers, as shown in Figure 5-49.

Figure 5-49 UCS E-Series NTP Servers



Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

PCI Assessment Detail—PCI Sub-Requirements with Compensating Controls

No sub-requirements were failed.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Administration

Authentication

Cisco Secure Access Control Server

Cisco Secure Access Control Server (ACS) was used as a central authentication system for the majority of products validated in this solution. It links user authentication to Windows Active Directory using group mapping that segments users based on their role and function.

Cisco Secure ACS is an access policy control platform that helps you comply with growing regulatory and corporate requirements. By using a single authentication method for all system devices, insight into who made changes is simplified for internal administration, assessors, and post-breach audits. It supports multiple scenarios simultaneously, including the following:

- Device administration—Authenticates administrators, authorizes commands, and provides an audit trail
- Remote access—Works with VPN and other remote network access devices to enforce access policies
- Wireless—Authenticates and authorizes wireless users and hosts and enforces wireless-specific policies
- Network admission control—Communicates with posture and audit servers to enforce admission control policies

Cisco Secure ACS lets you centrally manage access to network resources for a growing variety of access types, devices, and user groups. These key features address the current complexities of network access control:

- Support for a range of protocols including Extensible Authentication Protocol (EAP) and non-EAP protocols provides the flexibility to meet all your authentication requirements
- Integration with Cisco products for device administration access control allows for centralized control and auditing of administrative actions
- Support for external databases, posture brokers, and audit servers centralizes access policy control and lets you integrate identity and access control systems

Table 5-18 PCI Assessment Summary—Cisco Secure Access Control Server

Models Assessed	
Cisco Secure Access Control Server	Release 4.2(1) Build 15 Patch 3
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of Cisco Secure ACS is to securely authenticate users to the systems within the cardholder environment.

Table 5-19 lists the component assessment details for Cisco Secure ACS.

Table 5-19 Component Capability Assessment—Cisco Secure ACS



Cisco Secure ACS

PRIMARY FUNCTION
Securely authenticate users to systems in the cardholder environment

REQUIREMENT: 7, 8 (7.1, 7.2, 8.2)

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
✓	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
✓	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Cisco Secure ACS has been configured to authenticate individual users using Active Directory (AD). This is accomplished by creating user groups in AD and mapping them to role-based groups in Cisco Secure ACS. This provides the granularity of secure authentication needed to address the PCI specification.
- The solution used the windows versions of Cisco Secure ACS. The CSA client was installed to protect and alert on unauthorized access of the log and audit trail.
- Remove the default accounts for administration.
- Enable HTTPS and disable HTTP.
- User authentication services for Cisco Secure ACS are linked to a centralized Active Directory user database

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*

If Cisco Secure ACS is deployed on a server, it should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

If Cisco Secure ACS is deployed as an appliance, no unnecessary services are enabled by default.

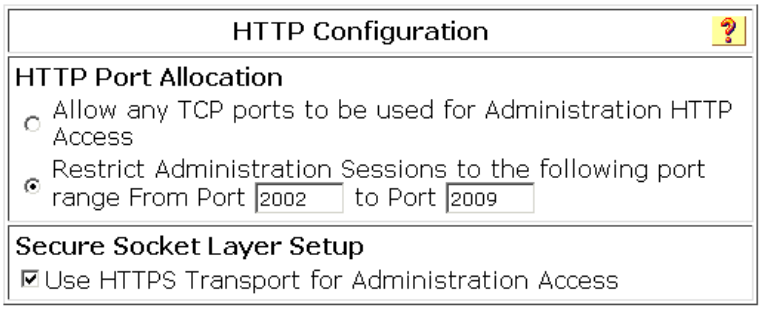
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Secure ACS should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

  If Cisco Secure ACS is deployed as an appliance, no unnecessary services are enabled by default.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The management console was configured to support HTTPS access, with HTTP access disabled. Cisco Secure ACS is configured to use SSL as a highly secure management portal technology (see Figure 5-50). Cisco Secure ACS employs port hopping to a random high port for secured communication transport.

Figure 5-50 HTTP Configuration



Note Server hardening, including appropriate security settings for all system components, is the responsibility of the organization/service provider.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Secure ACS. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the Cisco Secure ACS internal database for administrator users. Within Cisco Secure ACS, individual administrative user IDs were created and assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco Secure ACS includes extensive controls for defining user privileges and by default denies access to all individuals without a system User ID.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database as shown below.

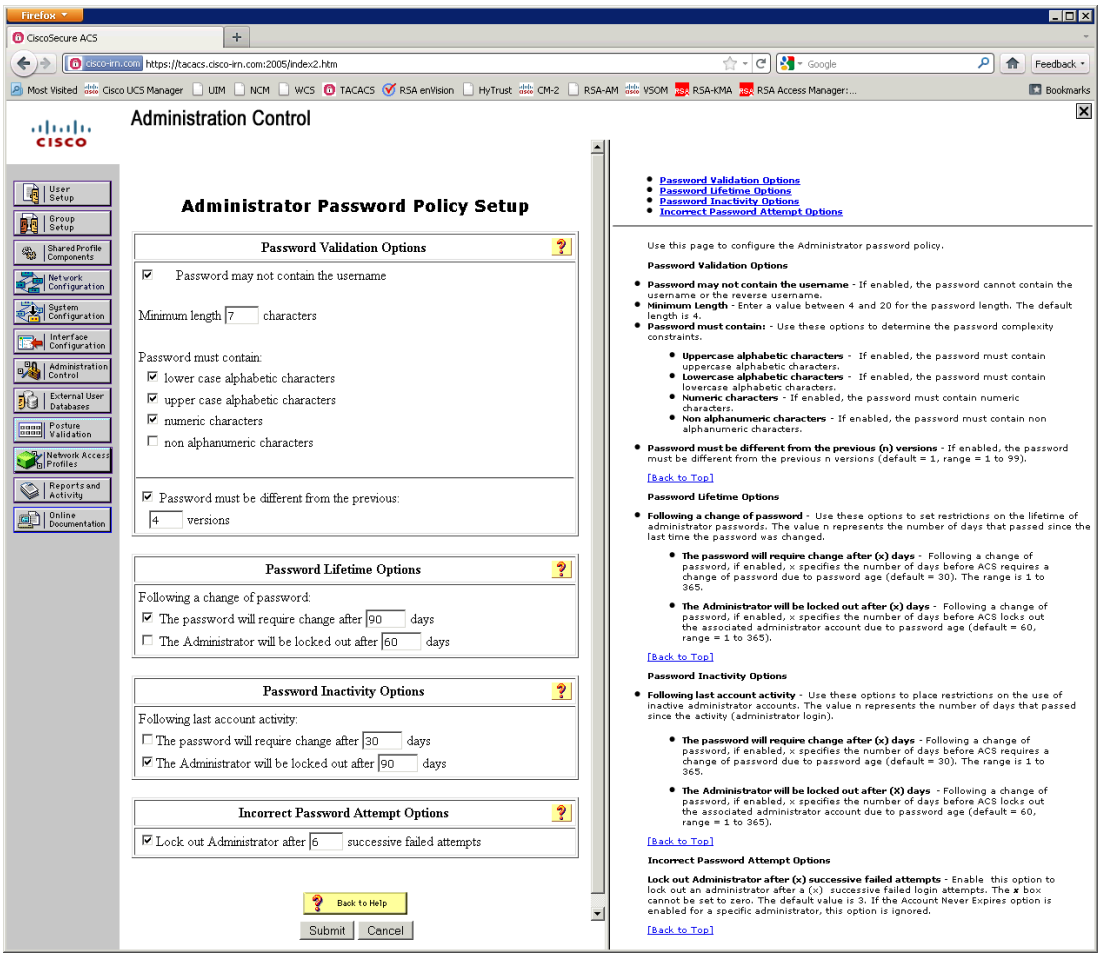
- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco Secure ACS supports the creation of local users. Through company policy, each user must be assigned a unique ID.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local administrator user accounts in Cisco Secure ACS require setting of a password according to the password requirements, as shown in Figure 5-51.

Figure 5-51 Administrator Password Requirements



- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Passwords are not readable within Cisco Secure ACS; it uses strong cryptography.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Through company policy inactive users should be removed or disabled every 90 days. As shown in Figure 5-51, Cisco Secure ACS password policy also enables setting of an inactivity option where an administrator will be locked out after 90 days of inactivity.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  The password lifetime option must be enabled configured to require users to change their password every 90 days. This setting can be configured as shown in Figure 5-51.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The default password policy for length specifies a minimum password length of 4 characters; this must be changed to 7 characters, as shown in Figure 5-51.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The password policy must be updated to require both alphabetic and numeric characters, as shown in Figure 5-51.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The password history option must be enabled and configured and set to 4 versions, as shown in Figure 5-51.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  The Incorrect Password Attempt Options must be enabled and the default of 3 attempts must be changed to 6 successive failed authentications attempts, as shown in Figure 5-51.

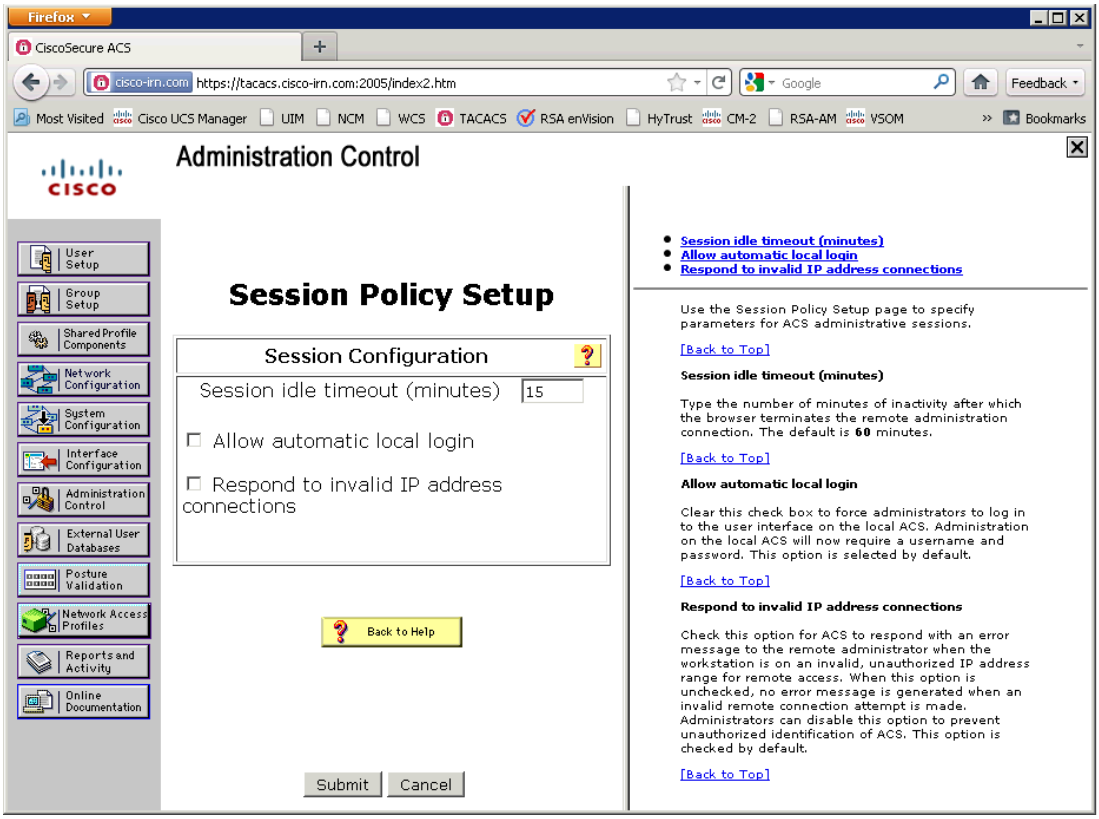
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  By default, Cisco Secure ACS requires another administrator to re-enable locked out accounts.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco Secure ACS supports session policies under the Administration Control/Session tab. Change the Session Time-out to 15 minutes from the default 60 minutes, as shown in Figure 5-52.

Figure 5-52 Session Timeout



Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Secure ACS is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*

- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Secure ACS uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4**—*Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

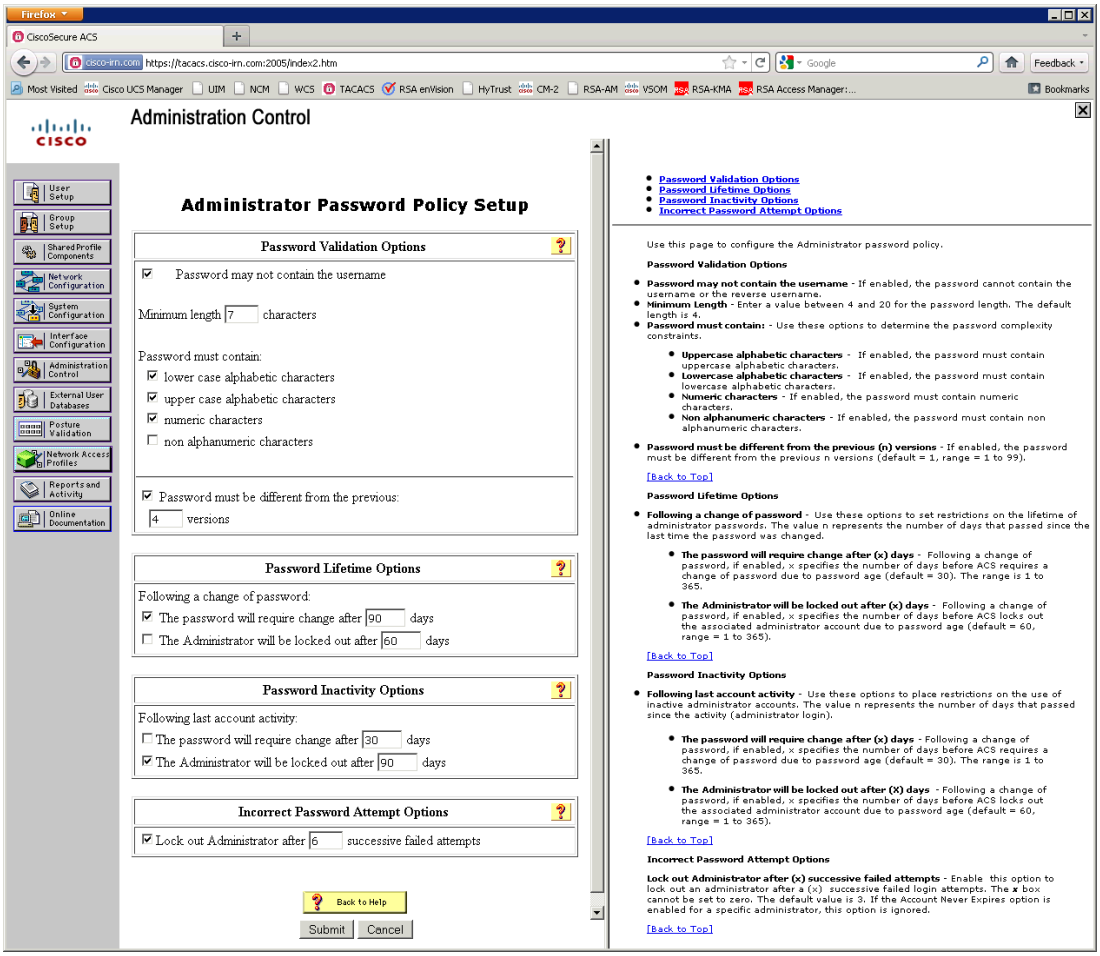
Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

Cisco Secure ACS can be configured to send its log data to the RSA enVision log management platform to meet the above requirements. The configuration procedure is documented in the RSA enVision Event Source Configuration Guide for Cisco Secure ACS, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/).

RSA enVision requires that specific attributes for each reporting function to be specified and configured in a particular order. Figure 5-53 shows the required items for generating Syslog Passed Authentications. Settings for other event types are available in the RSA enVision Event Source Configuration Guide for Cisco Secure ACS.

Figure 5-53 Syslog for Passed Authentications



PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

RSA Authentication Manager

RSA Authentication Manager is the management component of the RSA SecurID®, a two-factor authentication solution, which provides a much more reliable level of user authentication than reusable passwords. SecurID authentication is based on something you know (a password or PIN) and something you have (an authenticator), and can be used to achieve compliance to PCI requirement 8.3, which requires two-factor authentication for remote access to the network by employees, administrators, and third parties. As the management component, RSA Authentication Manager is used to verify authentication requests and centrally administer authentication policies for enterprise networks.

Table 5-20 PCI Assessment Summary—RSA Authentication Manager

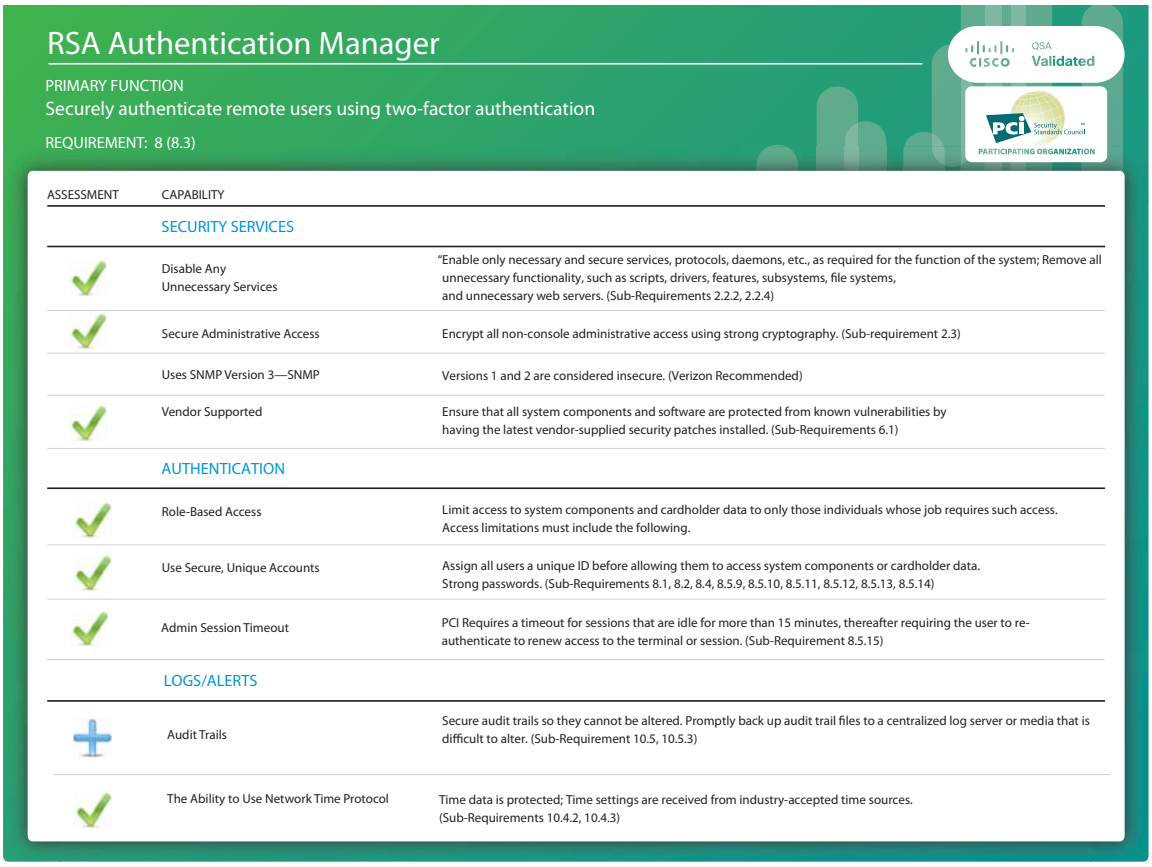
Models Assessed	
RSA Authentication Manager 7.1 Service Pack 2	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.3, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of RSA Authentication Manager is to securely authenticate remote users using two-factor authentication.

Table 5-21 lists the component assessment details for RSA Authentication Manager.

Table 5-21 Component Capability Assessment—RSA Authentication Manager



RSA Authentication Manager

PRIMARY FUNCTION
Securely authenticate remote users using two-factor authentication

REQUIREMENT: 8 (8.3)

CISCO QSA Validated

PCI Security Standards Council PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
✓	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
✓	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

RSA Authentication Manager stores and processes highly sensitive authentication information and should be deployed and operated in a secure manner. Detailed recommendations are found in the RSA Authentication Manager Security Best Practices Guide, which can be downloaded from RSA Secure Care Online (https://knowledge.rsasecurity.com/).

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are no unnecessary services enabled by default on RSA Authentication Manager. RSA Authentication Manager should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  RSA Authentication Manager should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  RSA Authentication Manager web consoles are protected with SSL.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  RSA Authentication Manager publishes security patches on RSA Secure Care Online (https://knowledge.rsasecurity.com/) in accordance with industry best practices to manage and respond to security vulnerabilities to minimize customers' risk of exposure.

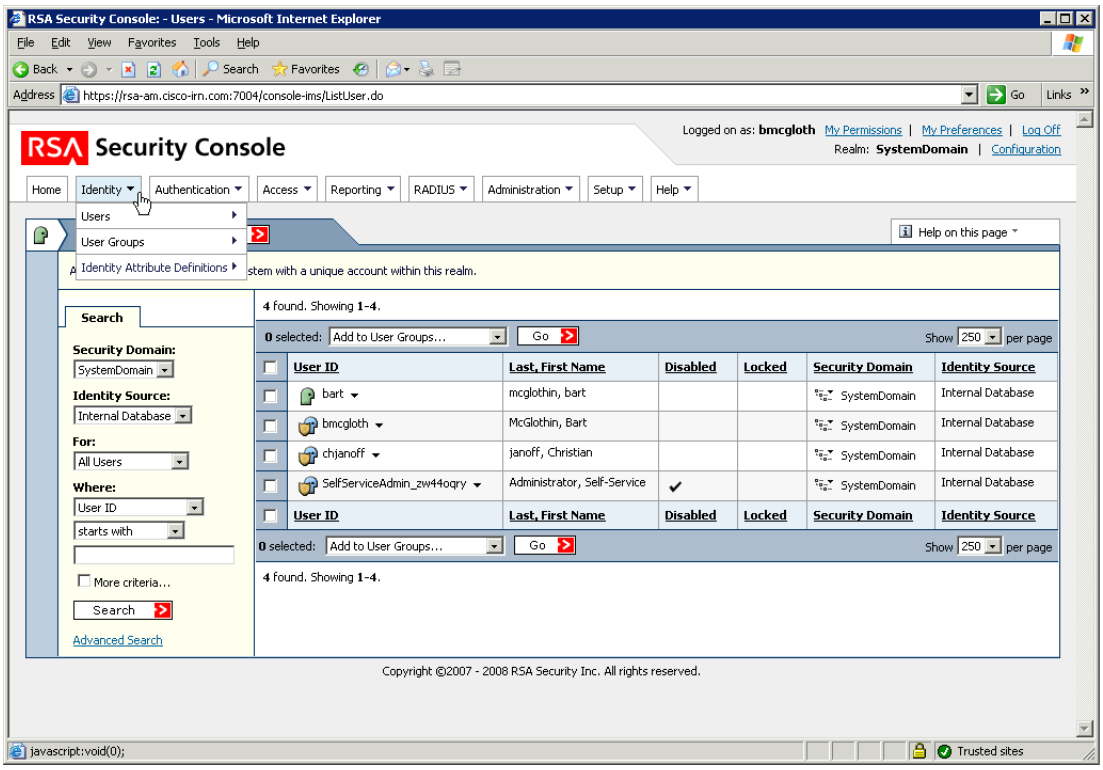
Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the RSA Authentication Manager's internal database. RSA Authentication Manager also supports linking to a centralized user database such as Active Directory using LDAP. Within RSA Authentication Manager, individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

RSA Authentication Manager has powerful access control capabilities to limit access to system components and cardholder data based on user role or group membership. Users and groups are created under the Identity tab of the Security console, as shown in Figure 5-54.

Figure 5-54 Users and Groups



- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

RSA Authentication Manager's access control system defaults to deny access.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database as shown below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

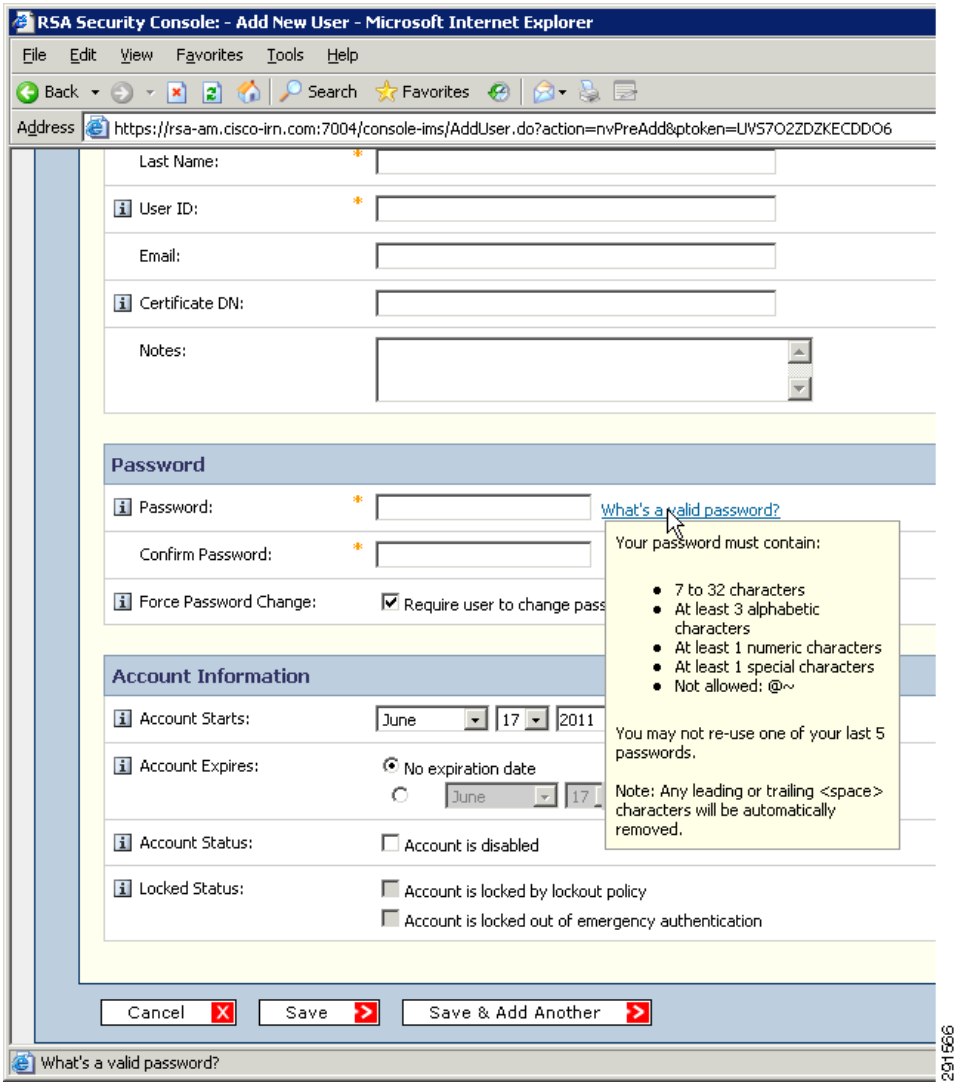
  RSA Authentication Manager supports the creation of local users or linking to a central repository of users. Through company policy, each user must be assigned a unique ID.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*

  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

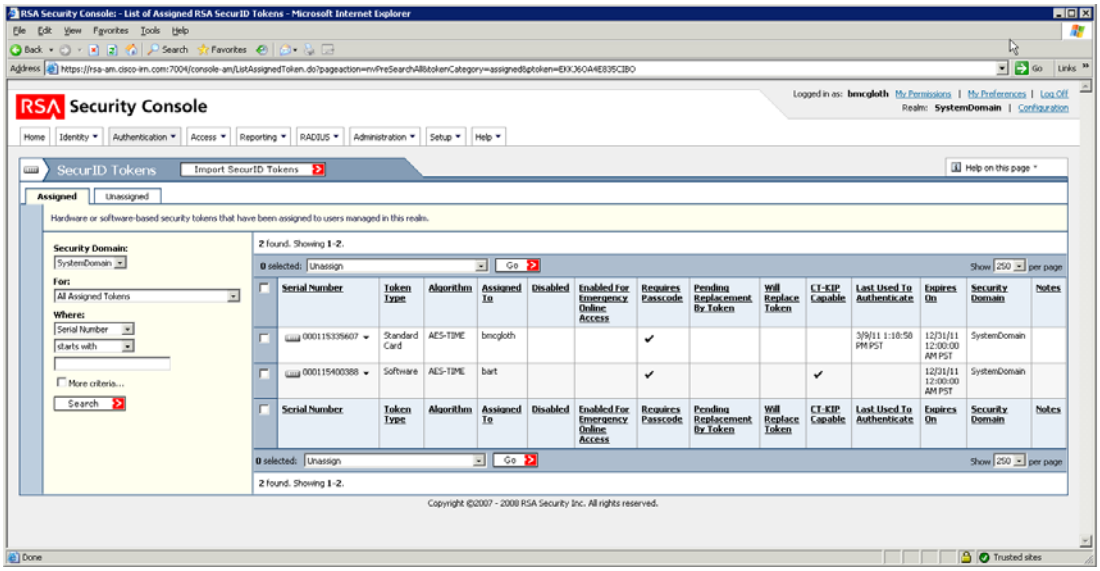
  Local user accounts in RSA Authentication Manager require setting of a password according to the assigned password policy as shown in Figure 5-55.

Figure 5-55 User Password Requirements Based on Policy



Additional authentication tokens can also be assigned to each user, as shown in Figure 5-56.

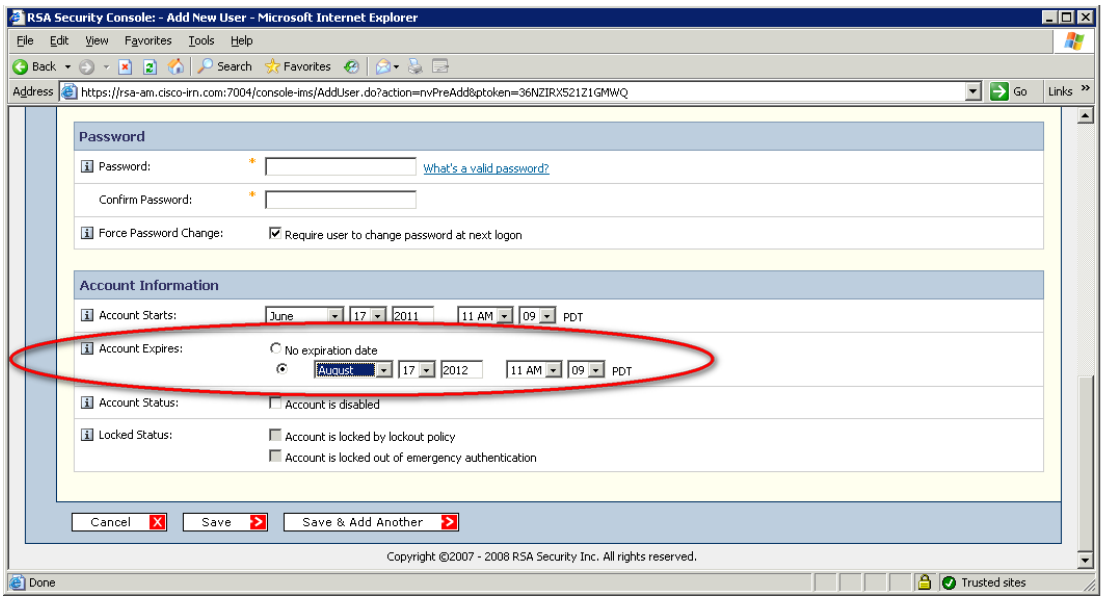
Figure 5-56 Assigned Tokens



- **PCI 8.3**—*Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Through company policy, inactive users should be removed or disabled every 90 days. RSA Authentication Manager also enables setting of an account expiration date for individual accounts, as shown in Figure 5-57.

Figure 5-57 User Account Expiration



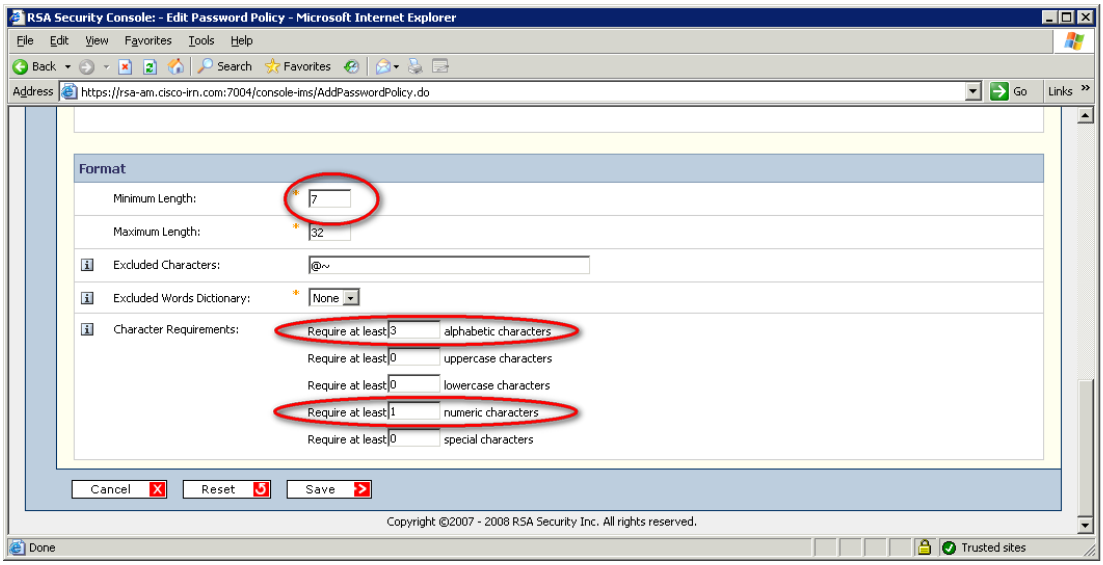
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  The default Initial Password Policy is created when a new realm is established, and requires users to change their passwords every 90 days.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The default Initial Password Policy must be updated to set a minimum password length of 7 characters, as shown in Figure 5-58.

Figure 5-58 Initial Password Policy



- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The default Initial Password Policy must be updated to require both alphabetic and numeric characters, as shown in Figure 5-58.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The default Initial Password Policy is created when a new realm is established, and restricts users from re-using their last five passwords.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

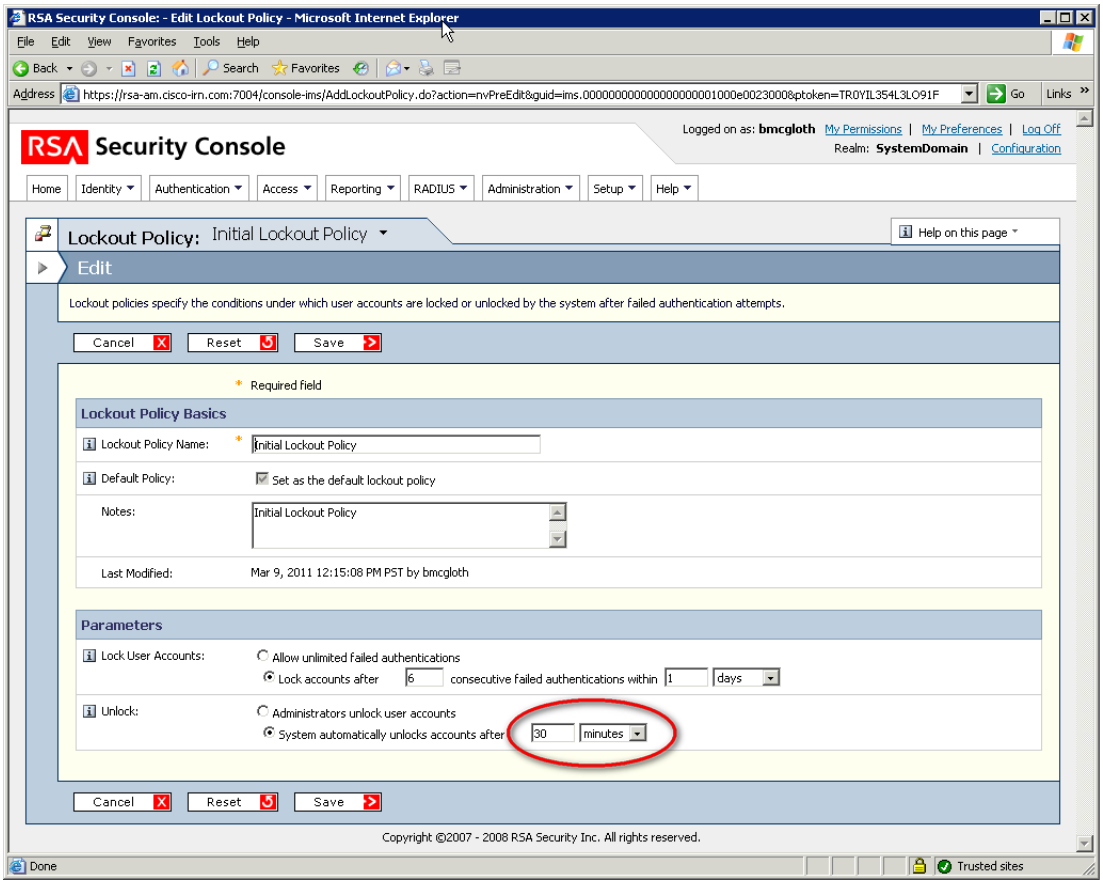
  The Initial Lockout policy is enabled by default and locks accounts after six consecutive failed authentications within one day.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  The Initial Lockout policy is enabled by default; the only change for PCI compliance is to change the auto-unlock parameter from 15 minutes to 30 minutes. This change is made under the Authentication > Policies > Lockout Policies.

  Figure 5-59 shows an appropriate policy for PCI compliance.

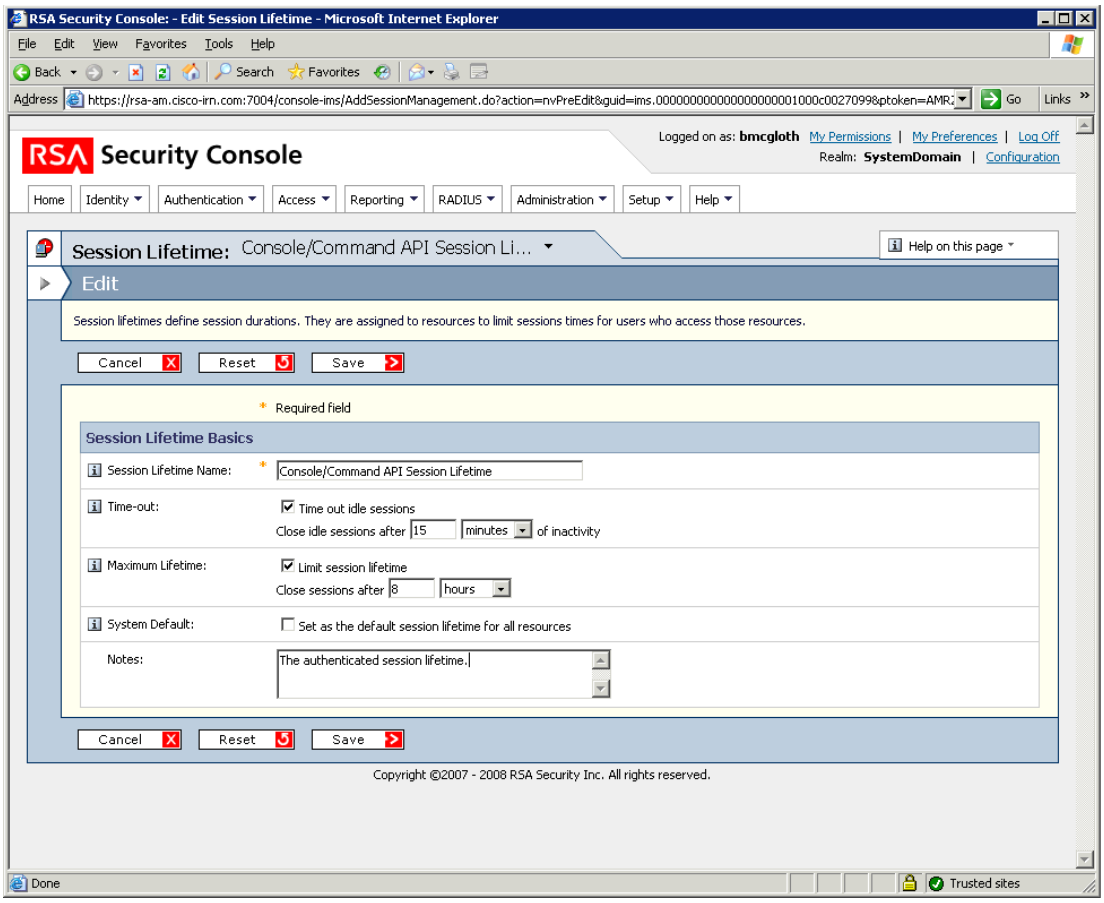
Figure 5-59 Revised Initial Lockout Policy Edited for PCI



- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  RSA Authentication Manager supports session policies under the Access tab. Change the Session Time-out for the Console/Command API to 15 minutes from the default, as shown in Figure 5-60.

Figure 5-60 Session Lifetime for Console



RSA Authentication Manager has very powerful and flexible capabilities to define password and account lockout policies to meet all of the above criteria.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

RSA Authentication Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*

- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

RSA Authentication Manager uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

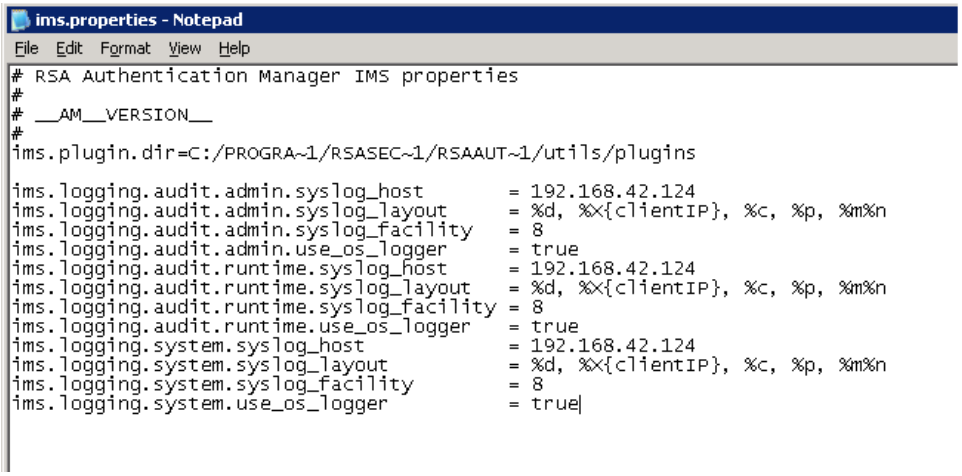
- **PCI 10.5**—*Secure audit trails so they cannot be altered.*

  Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  RSA Authentication Manager can be configured to send its log data to the RSA enVision log management platform to meet the above requirements. The configuration procedure is documented in the enVision Event Source Configuration Guide for RSA Authentication Manager, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/). One step is editing the IMS.Properties file, as shown in Figure 5-61.

Figure 5-61 IMS Properties File



PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Identity Services Engine

Cisco Identity Services Engine (ISE), a security component of the Cisco Borderless Network architecture, provides visibility and control into who and what is connected to the network. Cisco ISE allows organizations to embrace the rapidly changing business environment of mobility, virtualization, and collaboration while enforcing compliance, maintaining data integrity and confidentiality, and establishing a consistent global access policy. Cisco ISE allows businesses to gain complete control over the access points into their networks. This includes all wired, wireless, and VPN network entry points.

Cisco ISE ensures that you know what devices and users are on your network, and that those devices and users comply with your security policies via the following components:

- Cisco Identity Services Engine—A next-generation policy manager that delivers authentication, authorization, and accounting (AAA); posture; profiling; and guest management services on a single platform. The Cisco ISE automatically discovers and classifies endpoints, provides the right level of access based on identity, and provides the ability to enforce endpoint compliance by checking a device's posture. The Cisco ISE also provides advanced authorization and enforcement capabilities, including Security Group Access (SGA) through the use of security group tags (SGTs) and security group access control lists (ACLs). Administrators can centrally create and manage access control policies for users and endpoints in a consistent fashion, and gain end-to-end visibility into everything that is connected to the network.
- Cisco ISE Identity on Cisco Networking Infrastructure—Identity-based networking services on the Cisco routing, switching, and wireless infrastructure provides the ability to authenticate users and devices via features such as 802.1x, MAC authentication bypass, and web authentication. In addition, this same infrastructure is what enforces the appropriate access into parts of the network via VLANs, downloadable or named ACLs and security group ACLs.

- Client—Cisco Anyconnect is a software client that enables you to deploy a single 802.1x authentication framework to access wired and wireless networks while the Cisco NAC agent delivers endpoint posture information. The Cisco ISE architecture also supports native O/S supplicants.

The Cisco Identity Services Engine solution offers the following benefits:

- Allows enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise
- Prevents unauthorized network access to protect corporate assets
- Provides complete guest lifecycle management by empowering sponsors to on-board guests, thus reducing IT workload
- Discovers, classifies, and controls endpoints connecting to the network to enable the appropriate services per endpoint type
- Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention
- Offers a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations.

Figure 5-62 shows an example of a Cisco ISE-based LAN deployment.

Figure 5-62 Cisco ISE-Based LAN Deployment

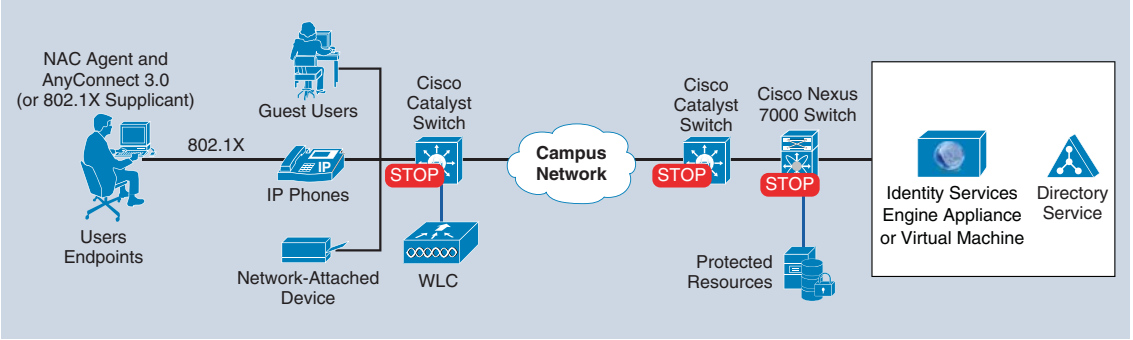


Table 5-22 PCI Assessment Summary—Cisco Identity Services Engine

Models Assessed	
Cisco Identity Service Engine version 1.2	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 9	9.1.2
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.4
PCI 11	11.1.b, 11.1.d
PCI Sub-Requirements Requiring Compensating Controls	

Table 5-22 PCI Assessment Summary—Cisco Identity Services Engine (continued)

No compensating controls were required to satisfy any sub-requirements.
PCI Sub-Requirements Failed
No sub-requirements were failed.

Primary PCI Function

Cisco ISE identity features detect and prevent rogue wireless devices from connecting to in-scope PCI networks (11.1); in addition, Cisco ISE locks down publicly accessible network ports to only authorized devices and users (9.1.2). In addition to its primary focus, Cisco ISE can also help with compliance and enforcement of requirements 6.1, 7.1, 7.2, 8.3, 8.5, and 10.

Table 5-23 lists the component assessment details for the Cisco ISE Solution.

Table 5-23 Component Capability Assessment—Cisco ISE

Cisco ISE

PRIMARY FUNCTION
Authenticate and authorize users and endpoints via wired, wireless, and VPN

REQUIREMENT: 7, 11 (7.1, 7.2, 11.1)

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
✓	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

For the purposes of this guide, Cisco ISE is configured to authenticate individual users and ISE Admin users using Active Directory (AD). Cisco ISE is also used to profile and assess the posture of individual wired and wireless devices to ensure that they comply with the PCI standard. Cisco ISE relies on TrustSec wired and wireless identity features such as 802.1x, MAB, and web portal authentication on Cisco infrastructure to collect user identity information. It relies on the Cisco ISE NAC agent and the Cisco ISE profiler engine to collect posture and profiling information from devices.

Note the following ISE configuration best practices for PCI compliance:

- The solution tested used the virtual machine appliance version of Cisco ISE running on an ESX platform.
- The default accounts for administration are removed.
- ISE only supports HTTPS and SSH access
- Cisco ISE communicates with the Cisco switches and wireless controllers using RADIUS.
- Cisco ISE can use dynamic VLAN and port or VLAN access control rules to provide PCI segmentation of a network. For example, members of the PCI active directory group are automatically moved to the PCI VLAN when they connect to the network. Cisco ISE can then apply strong access lists to this VLAN or directly to the user switch port to accomplish segmentation.
- Access control rule sets must adhere to a "least amount of access necessary" policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment on the point-of-sale networks.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- The Cisco ISE system is configured to be compliance with all of the access controls, logging controls, and other general system controls required by PCI DSS 2.0.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure. (For example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.)*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

  The Cisco Identity Service Engine appliance does not allow changes to the operating system, to the database, installation of unsupported hardware, or of unsupported third-party software.

  The Cisco ISE management console supports only HTTPS access.

  Cisco ISE is configured to use SSL as a highly secure management portal technology.

  Role-based administration is configured for administrative tasks.

  Cisco ISE was locked down according to generally accepted industry standards and the above PCI requirements.

Figure 5-63 Admin Access Using Active Directory for Authentication



Requirement 6: Develop and maintain secure systems and applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.*

Note An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices, systems, and databases) and higher than less-critical internal devices, ensuring that high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.

Cisco ISE can be upgraded and patched manually.

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in the Cisco Identity Service Engine. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html

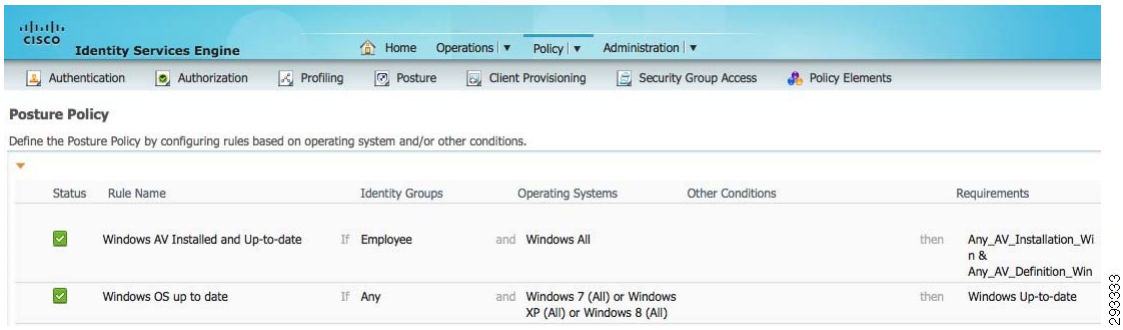
The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

ISE is used for ensuring network-wide compliance with PCI 6.1 for all Windows and Mac OSX systems. Systems are posture-assessed for compliance upon connection to the network. If found not to be compliant, remediation and access restrictions can be put in place on the network.

Cisco ISE is able to check all hosts connecting to the network to make sure they are compliant with requirement 6.1. Cisco ISE has several auto-update configuration options you can use to keep its posture assessment database current. Operating system patches and application patches can be enforced before allowing network access. Cisco ISE can offer remediation options to users who are out of compliance. In addition to OS updates, ISE can also ensure anti-virus software is installed, running and up to date.

Figure 5-64 ISE Endpoint Posture Policy for Checking AV and OS Compliance



Requirement 7: Restrict access to cardholder data by business need to know

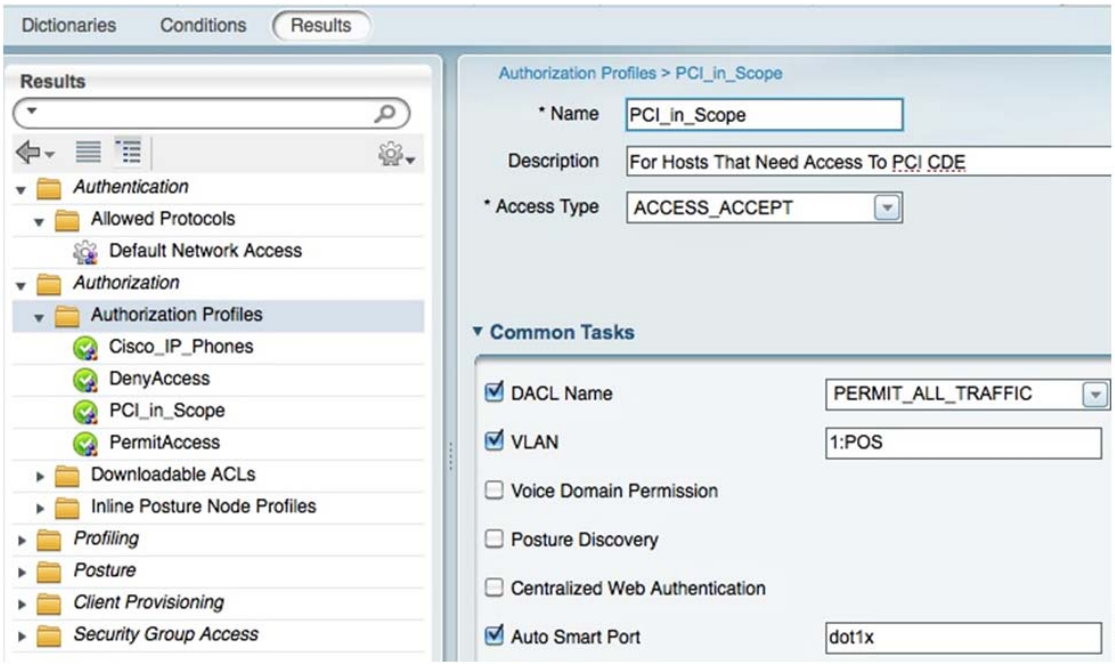
To meet all of the requirements listed below, the Cisco PCI Solution uses a centralized user database in the Active Directory. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. Cisco ISE connects to this resource via native Windows services to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function.*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system.*

ISE ensures that only privileged users can access the CDE. This is done using the authentication credentials supplied by the wired and wireless infrastructure, along with the AD attributes of a user connecting to the network. Based on a Cisco ISE authorization profile match, that user is put onto the proper VLAN and given a group-specific port access control list to control where they can go on the network. Additionally, a Cisco SmartPort macro can be run on the switchport to ensure they have the proper configuration.

Figure 5-65 shows the Authorization Profiles screen.

Figure 5-65 Authorization Profiles

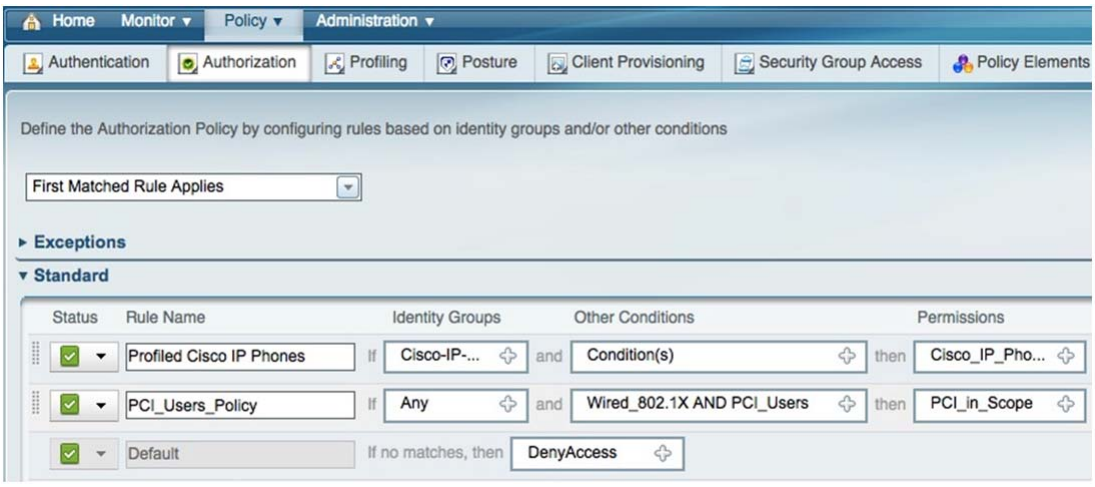


- **PCI 7.2.1**—*Coverage of all system components.*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function.*
- **PCI 7.2.3**—*Default "deny-all" setting.*

  If Cisco ISE does not explicitly match an authorization policy, network access is denied.

  Figure 5-66 shows the Authorization Policy screen.

Figure 5-66 Authorization Policy



Requirement 8: Assign a unique ID to each person with computer access

The relevant sub-requirements below were met using the Cisco ISE linked to the windows Active Directory domain. Cisco ISE also supports linking to other authentication servers.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco ISE supports the creation of local user accounts with unique IDs through the use of the **username** command in the CLI or via the Web GUI. These can be used for local fallback user accounts if connectivity to Active directory is lost.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  When configuring local user accounts, you must specify a password to achieve PCI compliance.

  Cisco ISE can use any of the methods indicated above to authenticate RADIUS users. The audited configuration for this guide used passwords stored on an Active directory server.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.* All local passwords on the Cisco ISE are stored using strong encryption

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco ISE supports tracking of a users last activity; accounts reviewed as having no activity can then be easily disabled or removed.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  The Cisco ISE password policy support the setting of a password expiration that forces the user to change their password every 90 days.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The Cisco ISE password policy is configurable to specify a minimum password length.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The Cisco ISE password policy is configurable to specify an appropriate complexity of numbers and characters.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

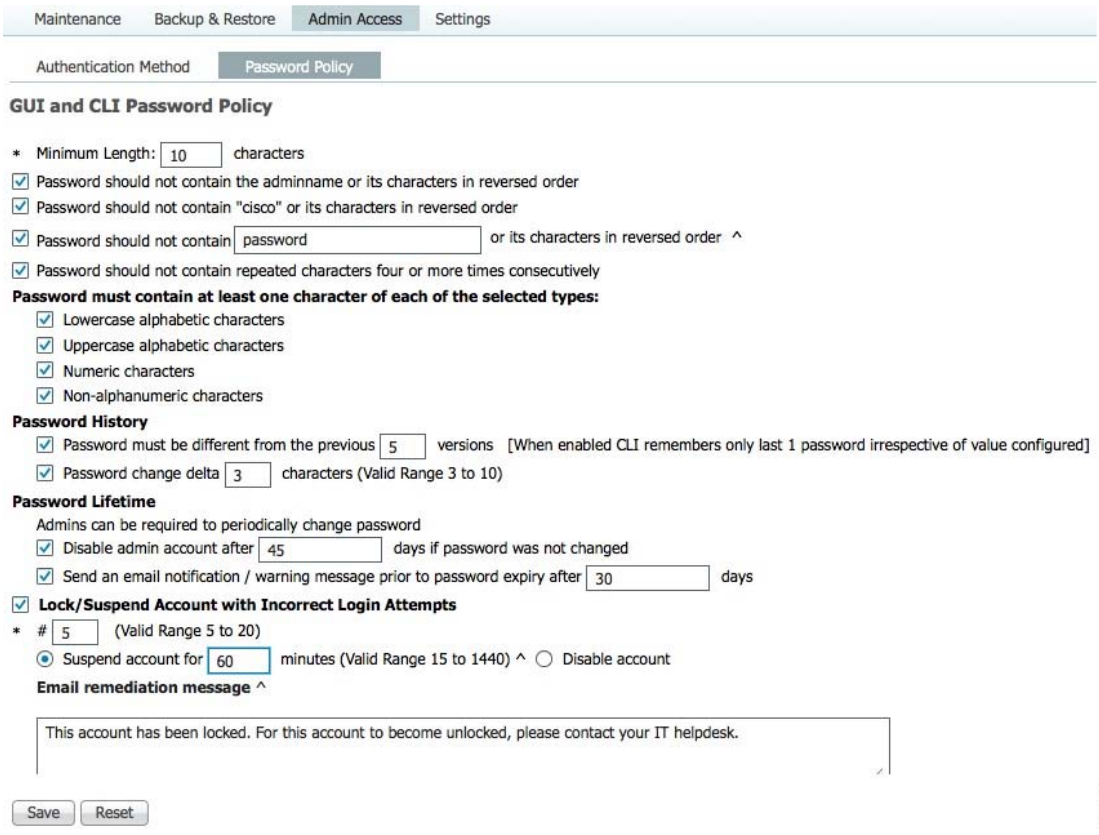
  The Cisco ISE password policy is configurable to track and prevent the re-use of historical password as configured in the Web GUI.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  ISE supports a robust administrator password policy and account lockout duration settings.

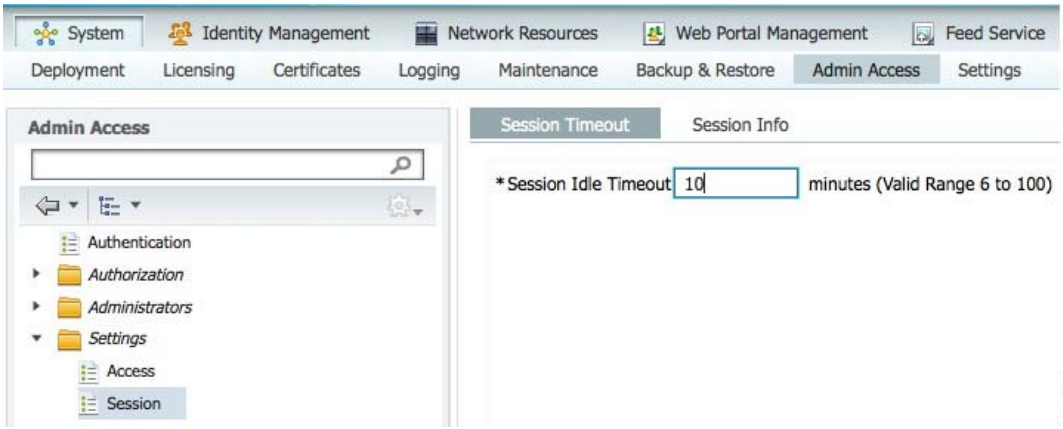
Figure 5-67 ISE Admin Password Policy Settings



- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco ISE is configured to re-authenticate both admin users and RADIUS users every 15 minutes.

Figure 5-68 Admin Access



Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.2**—*Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.*

  Cisco ISE can assist with this requirement by ensuring that all network jacks require AAA, posture assessment, and profiling. ISE can then determine the type of access to grant to that switchport based on the results of the above and/or based on the switchport's location. This type of authorization to the network would prohibit a non-authorized endpoint/user from access PCI data through publicly accessible network jacks.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco ISE uses the local clock facilities of the host server on which it is installed to meet the following requirements.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

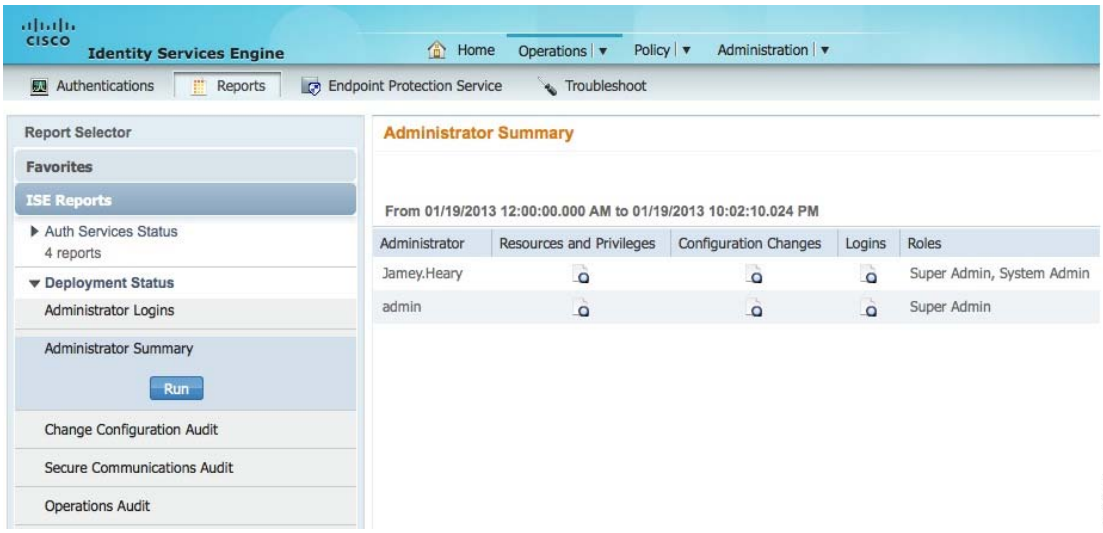
Cisco ISE uses the local clock facilities to meet the following requirements.

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco ISE uses NTP to meet these requirements by implementing the following configuration statement:

```
ntp server 192.168.62.161 192.168.62.162
```

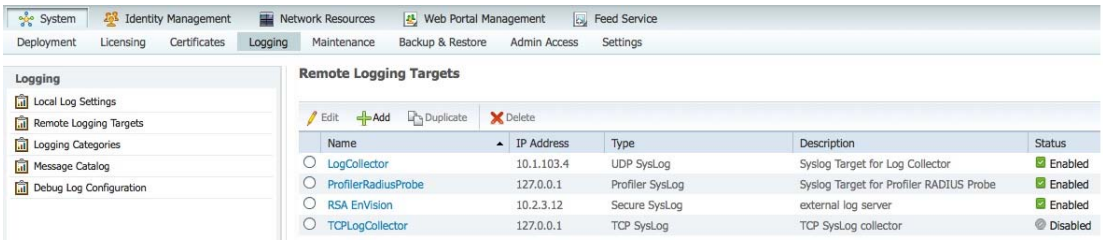
Figure 5-69 Administrator Summary



Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.4**—*Write logs for external-facing technologies onto a log server on the internal LAN.*

Figure 5-70 Remote Logging Targets



Requirement 11: Regularly test security systems and processes.

The following requirements can be addressed using Cisco network admission control.

- **PCI 11.1.b**—*Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:*
- *WLAN cards inserted into system components*
- *Portable wireless devices connected to system components (for example, by USB, etc.)*
- *Wireless devices attached to a network port or network device*
- **PCI 11.1.d**—*If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.*

Cisco ISE NAC capabilities can be configured on the store switches to automate the verification of approved devices being attached to the network. In addition to configuring the ISE authentication services in the data center, add the following configurations to all switch and switch interface ports where ISE network access control is required. In most cases, every access switch port in your network should be protected using ISE. However, as a minimum, any switchport that could potentially let a host find its way to the PCI security domain should be protected by Cisco ISE.

Pre-requirements for ISE NAC (domain name, name server, time settings, crypto keys):

```
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
Crypto key generate rsa 1024
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
clock timezone PST -8
clock summer-time PDT recurring
!
! ----Configurations to add for NAC ----
!
aaa new-model
!
!
aaa authentication dot1x default group radius local
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
client 192.168.42.111
server-key 7 <removed>
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
radius-server vsa send accounting
radius-server vsa send authentication
!
authentication mac-move permit
!
!
ip device tracking
ip admission name ise proxy http inactivity-time 60
!
cts sxp enable
cts sxp default source-ip 10.10.111.13 {use Switch Management IP}
!
dot1x system-auth-control
!
fallback profile ise
  ip access-group ACL-DEFAULT in

   ip admission ise
    !
    ! ----Auto Smart Ports Macro method for port configurations-------
    !
    macro name dot1x
     switchport access vlan 11
     switchport mode access
     switchport voice vlan 13
     ip arp inspection limit rate 1000
     ip access-group ACL-DEFAULT in
```

```
authentication event fail action next-method
authentication host-mode multi-auth
authentication open
authentication order dot1x mab webauth
authentication priority dot1x mab
authentication port-control auto
authentication timer reauthenticate server
authentication timer inactivity server
authentication violation restrict
authentication fallback ise
mab
snmp trap mac-notification change added
dot1x pae authenticator
dot1x timeout tx-period 5
```

Methods that may be used in the process include but are not limited to wireless network scans, physical site inspections, Network Access Control (NAC), or wireless IDS/IPS.

Cisco ISE Identity features were enabled on the wired infrastructure to authenticate users and devices. The Cisco ISE Policy Manager was configured to not allow an unauthorized access point to connect to the wired network. Cisco ISE was configured to alert and mitigate this rogue wireless threat.

Cisco ISE was configured to profile all devices connected to the network. Any access points detected were allowed only if they were in the approved list. All wired ports were set up to authenticate and posture-assess users and devices connecting to the network switches. The device posture assessment included checks for the setup of peer-to-peer wireless network and the setup of a wireless card as an access point on the device. If either of these were true, the device would be denied network access.

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Management

Cisco Prime LAN Management Solution (LMS)

Cisco Prime LAN Management Solution (LMS), a part of Cisco Prime Infrastructure, delivers powerful network lifecycle management by simplifying the configuration, compliance, monitoring, troubleshooting, and administration of Cisco networks. Cisco Prime LMS offers end-to-end management for Cisco's latest business-critical technologies and services such as Medianet, Cisco ISE, and Cisco EnergyWise while ensuring compliance with corporate and regulatory requirements.

Table 5-24 PCI Assessment Summary—Cisco Prime LMS

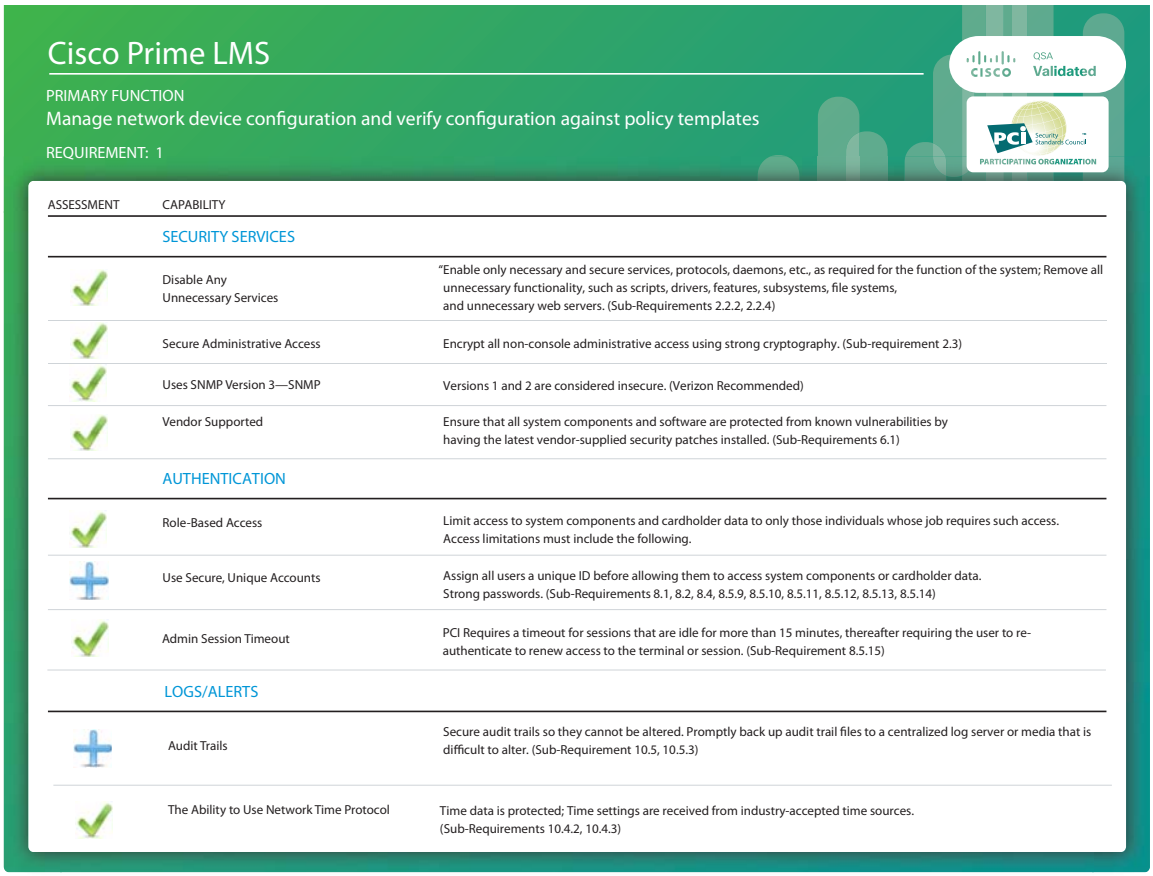
Models Assessed	
Cisco Prime LMS version 4.2.2	
PCI Sub-Requirements Passed	
PCI 1	1.2.2
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

LMS simplifies compliance by ensuring that all of the devices across the network adhere to the security policy of the company. In addition, it will verify that device configurations; match templates, are synchronized, and includes a customized PCI compliance dashboard to simplify the ongoing management for administrators (1.2.2).

Table 5-25 lists the component assessment details for the Cisco Prime LMS.

Table 5-25 Component Capability Assessment—Cisco Prime LMS



Cisco Prime LMS

PRIMARY FUNCTION
Manage network device configuration and verify configuration against policy templates

REQUIREMENT: 1

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
✓	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Provide sufficient licenses to cover all devices in your network.
- Provide proper host system sizing including CPUs, memory, and storage for the selected operating system.
- Restrict access behind a firewall or access list to only those administrative clients that need access.
- Activate the NMC capability license for compliance audits.

Compliance and Audit

The compliance and audit reports provide the compliance status of the network, lifecycle, and contract information about network devices, security advisory, and service reports based on device and software capabilities, and the services that are enabled.

The compliance reports provide information about the compliance state of the network for specific compliance requirements and can be found in LMS by navigating to Reports > Compliance and Audit.

Licensed/Unlicensed Compliance and Audit Reports

The following compliance and audit reports require a regulatory compliance management license:

- HIPAA Compliance Reports

- SOX (COBIT) Compliance Reports
- ISO/IEC 27002 Compliance Reports
- NSA Compliance Reports
- PCI DSS Compliance Reports
- DHS Checklist Reports
- DISA Checklists Report
- CIS Benchmarks

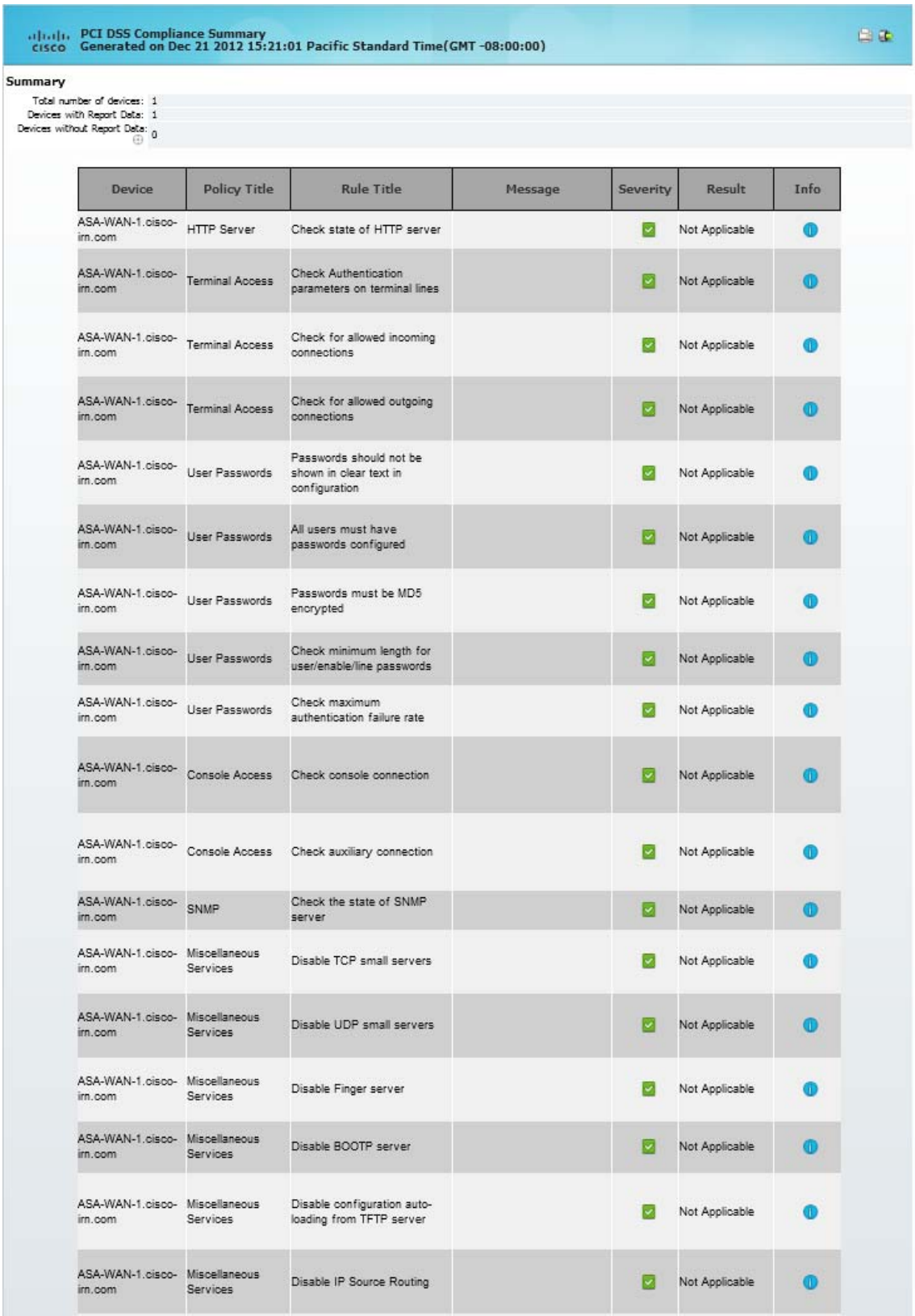
The following compliance and audit reports are supported by the LMS license alone and do not require a regulatory compliance management license:

- Service Reports
- Lifecycle Management Reports
- Vendor Advisory Reports
- Change Audit Reports

For compliance and audit license information, see the topic “Regulatory Compliance Management License in Administration with Cisco Prime LAN Management Solution 4.2.2”.

The Compliance and Audit Report module uses the stored configurations within the LMS database and evaluates them against specifically defined criteria of the selected devices. The PCI DSS Compliance Summary Report shows Payment Card Industry Data Security Standard (PCI DSS) security compliance audit results against either the entire network or selected network devices to verify how compliant the selected devices are against this regulation. (See Figure 5-71.)

Figure 5-71 PCI DSS Compliance Summary



PCI DSS Compliance Summary
Generated on Dec 21 2012 15:21:01 Pacific Standard Time(GMT -08:00:00)

Summary

Total number of devices: 1
Devices with Report Data: 1
Devices without Report Data: 0

Device	Policy Title	Rule Title	Message	Severity	Result	Info
ASA-WAN-1.cisco-irn.com	HTTP Server	Check state of HTTP server			Not Applicable	
ASA-WAN-1.cisco-irn.com	Terminal Access	Check Authentication parameters on terminal lines			Not Applicable	
ASA-WAN-1.cisco-irn.com	Terminal Access	Check for allowed incoming connections			Not Applicable	
ASA-WAN-1.cisco-irn.com	Terminal Access	Check for allowed outgoing connections			Not Applicable	
ASA-WAN-1.cisco-irn.com	User Passwords	Passwords should not be shown in clear text in configuration			Not Applicable	
ASA-WAN-1.cisco-irn.com	User Passwords	All users must have passwords configured			Not Applicable	
ASA-WAN-1.cisco-irn.com	User Passwords	Passwords must be MD5 encrypted			Not Applicable	
ASA-WAN-1.cisco-irn.com	User Passwords	Check minimum length for user/enable/line passwords			Not Applicable	
ASA-WAN-1.cisco-irn.com	User Passwords	Check maximum authentication failure rate			Not Applicable	
ASA-WAN-1.cisco-irn.com	Console Access	Check console connection			Not Applicable	
ASA-WAN-1.cisco-irn.com	Console Access	Check auxiliary connection			Not Applicable	
ASA-WAN-1.cisco-irn.com	SNMP	Check the state of SNMP server			Not Applicable	
ASA-WAN-1.cisco-irn.com	Miscellaneous Services	Disable TCP small servers			Not Applicable	
ASA-WAN-1.cisco-irn.com	Miscellaneous Services	Disable UDP small servers			Not Applicable	
ASA-WAN-1.cisco-irn.com	Miscellaneous Services	Disable Finger server			Not Applicable	
ASA-WAN-1.cisco-irn.com	Miscellaneous Services	Disable BOOTP server			Not Applicable	
ASA-WAN-1.cisco-irn.com	Miscellaneous Services	Disable configuration auto-loading from TFTP server			Not Applicable	
ASA-WAN-1.cisco-irn.com	Miscellaneous Services	Disable IP Source Routing			Not Applicable	

293310

PCI Assessment Detail—PCI Sub-Requirements Satisfied

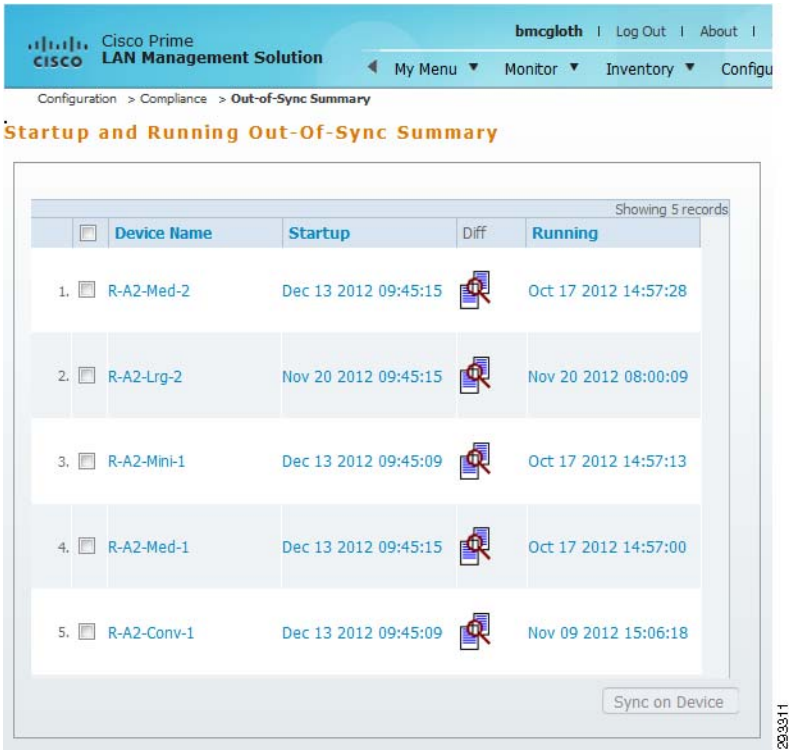
Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.2—***Secure and synchronize router configuration files.*

  Firewall, router, and switch configuration files are backed up centrally using Cisco Prime LMS. LMS automatically verifies that running and startup configurations of firewalls, routers, and switches are synchronized for the devices managed.

  The Out-Of-Sync Summary report can be used to view which systems configurations need to be synchronized and provides the ability to select and synchronize the devices. (See Figure 5-72.)

Figure 5-72 Out-of-Sync Summary Report

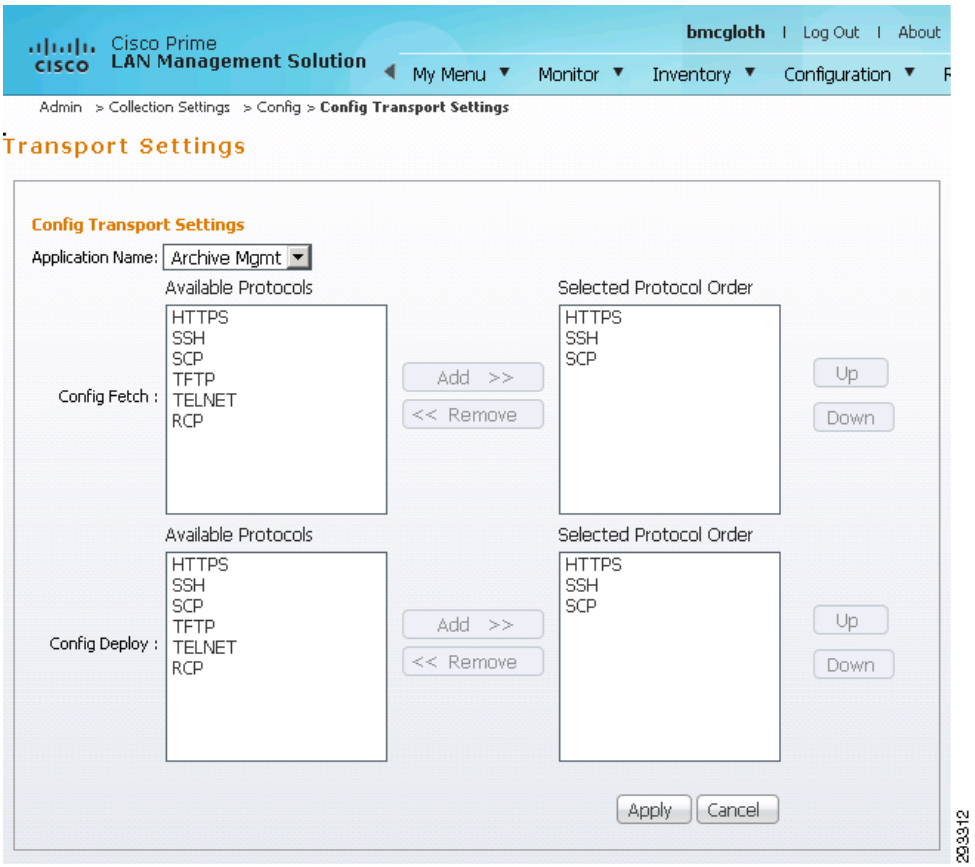


Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2—***Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2—***Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, and so on.*

  Cisco Prime LMS supports several protocols for securely managing devices. Device management preferences are configured in Admin > Collection Settings > Config> Config Transport Settings. Add secure protocols to the list in order of preference and remove insecure protocols for each Application Named function. Figure 5-73 shows the preferred protocol selections for Archive Management.

Figure 5-73 Device Management Transport Settings



- **PCI 2.2.4—***Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco Prime LMS soft appliance does not have any unnecessary services enabled by default.

  Cisco Prime deployed on other server platforms such as Windows or Solaris should first be hardened using industry best practices for those systems before installing the LMS application. Server hardening best practices guidelines can be found at a variety of Internet resources provided by the vendor or sites such as the NSA, NIST, and SANS.

- **PCI 2.3—***Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco Prime LMS supports encrypted administrative access via SSH and HTTPS. SSH is enabled by default after installation. HTTPS can be enabled with a self-signed certificate or public certificate. To enforce the use of only SSL for the web interface of LMS, perform the following configurations, as shown in Figure 5-74). These configuration steps can also be found in the LMS 4.2 Administration Guide, page 53.

Figure 5-74 Enable Cisco Prime LMS Browser Security



To enable browser-server security, complete the following steps.

Procedure

Step 1 Select **Admin > Trust Management(4.2.2 patch) > Local Server > Browser-Server Security Mode Setup**.

The Browser-Server Security Mode Setup dialog box appears.

Step 2 Select the **Enable** option to enable SSL.

Step 3 Click **Apply**.

Step 4 Log out from your Cisco Prime session and close all browser sessions.

Step 5 Restart the Daemon Manager from the LMS Server CLI.

On Windows:

a. Enter net stop crmdmgtd

b. Enter net start crmdmgtd

On Solaris/Soft Appliance:

a. Enter /etc/init.d/dmgtd stop

b. Enter /etc/init.d/dmgtd start

Step 6 Restart the browser and the Cisco Prime session.

When accessing the LMS CLI, you need to enter the SHELL by using the "shell" command. Then you can execute the stop/start commands for the soft appliance.

If you have issues logging in to LMS (lsuch as long delays), try disabling the launch of the LMS Getting Started page by default (as the first page after log in) by completing the following steps:

a. Open the properties file name “gs.properties” under the following path:

Windows:

/<<NMS-ROOT>>/MDC/tomcat/webapps/cwlms/WEB-INF/classes/com/Cisco/nm/gs/ui/gs.properties

Soft appliance:

./opt/CSCOpx/MDC/tomcat/webapps/cwlms/WEB-INF/classes/com/cisco/nm/gs/ui/gs.properties

b. Update the field IS_DEFAULT_PAGE as “false”.

c. Clear the browser cache and login-in (Daemon restart not required).

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

  For more information about PSIRT:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

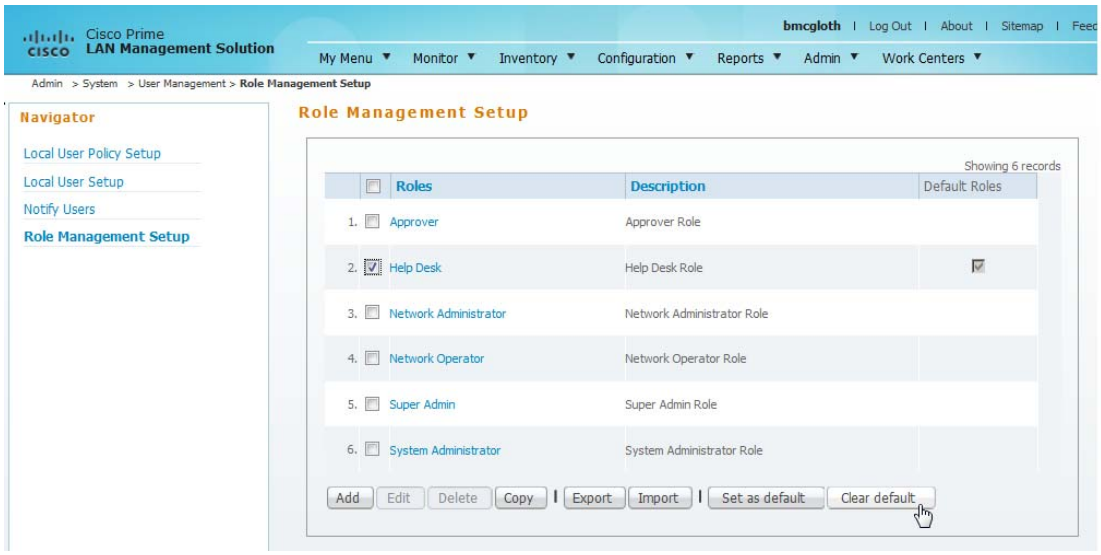
Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS using TACACS+ services. Individual user IDs are assigned. Roles are defined within LMS and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1—***Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2—***Assignment of privileges is based on individual personnel’s job classification and function*
- **PCI 7.1.3—***Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4—***Implementation of an automated access control system*
- **PCI 7.2.1—***Coverage of all system components*
- **PCI 7.2.2—***Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3—***Default “deny-all” setting. Note: Some access control systems are set by default to “allow-all,” thereby permitting access unless/until a rule is written to specifically deny it.*

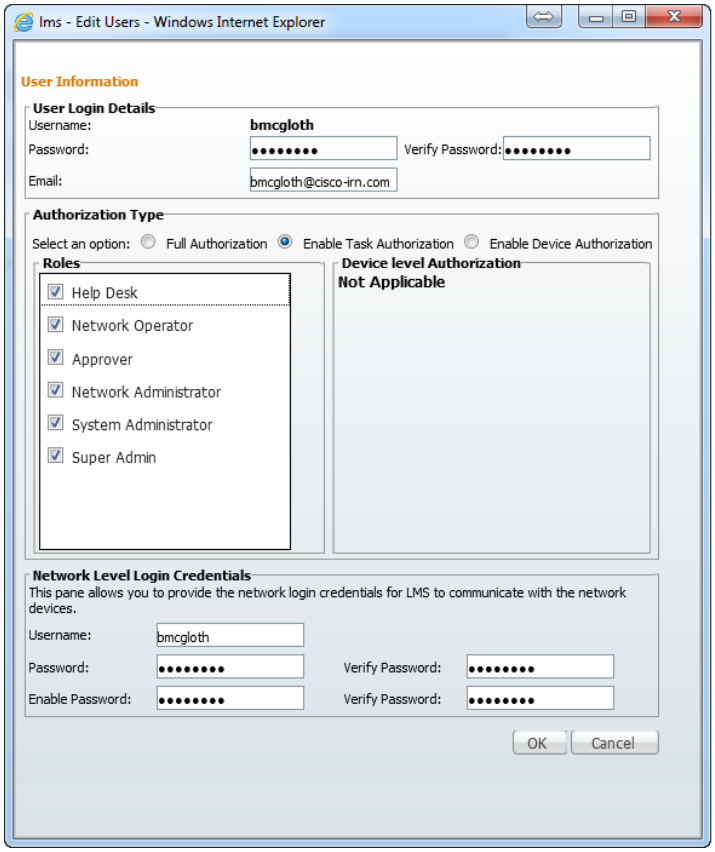
  Cisco Prime LMS supports role-based user access. Users can be assigned to role groups and, based on privilege levels, have access to only the tasks they require for their job function. By default in Cisco Prime LMS, authenticated users are allowed help desk level access unless specifically configured and assigned to appropriate roles. To restrict access to only configured users, clear the default role option under Admin > System > User Management > Role Management Setup (see Figure 5-75).

Figure 5-75 Role Management Setup



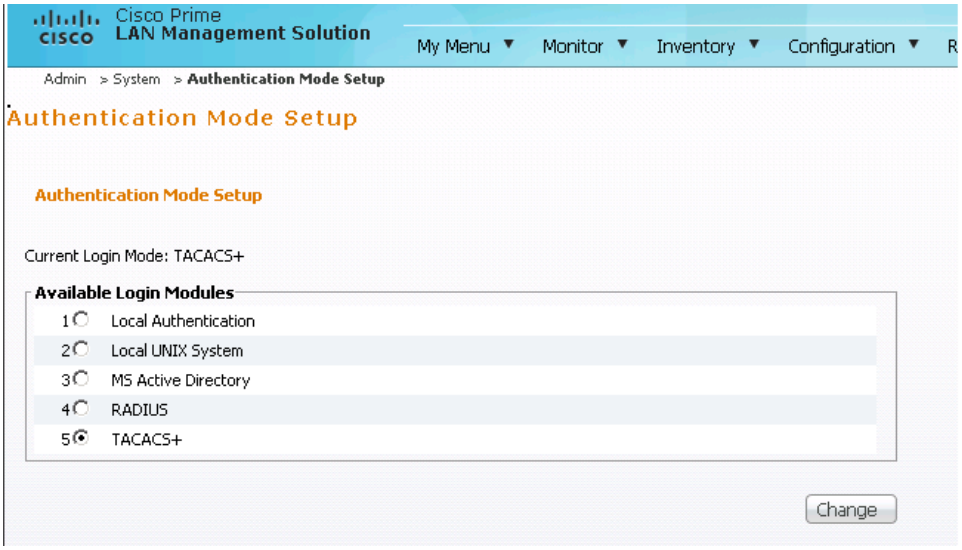
Local user accounts are configured to authorize role privileges and can also be used as fallback if the central authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8. (See Figure 5-76.)

Figure 5-76 LMS Local User Profile and Roles



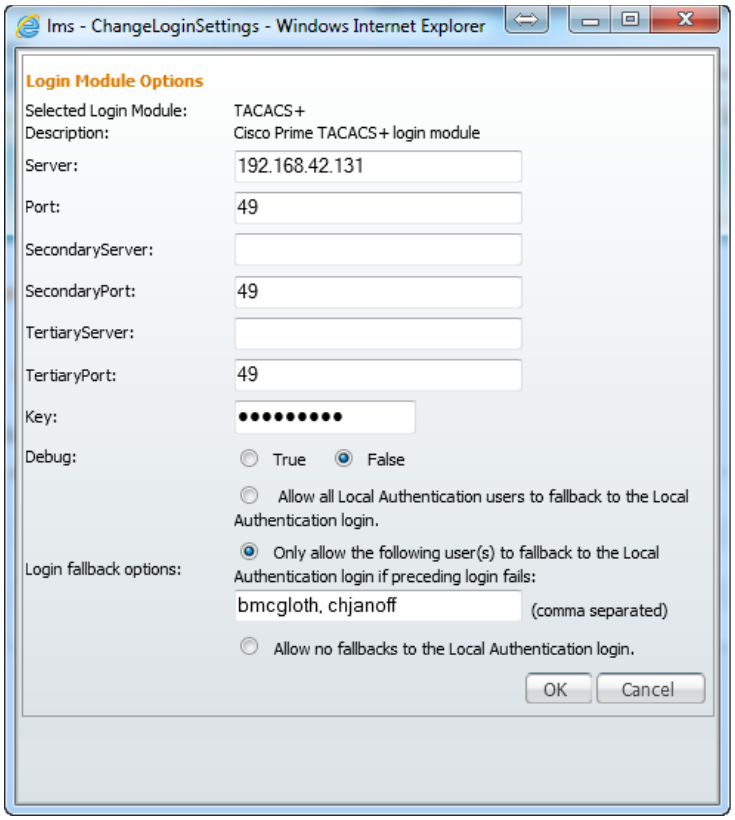
Several AAA services are available to externally authenticate users assigned to administer the system. Roles for these individuals are created and managed within the LMS system (see Figure 5-77). As of version 4, LMS no longer supports external authorization.

Figure 5-77 Authentication Mode Setup



In the TACACS server configuration, either all accounts or only specified accounts can be allowed for authenticaiton in the event that the ACS server cannot be reached. (See Figure 5-78.)

Figure 5-78 Login Module Options



Cisco LMS does not include the capability to restrict access to its CLI and HTTPS interfaces from only authorized systems. This server should be implemented in a network segment that includes firewalling or access list restriction capabilities to ensure proper access is limited as necessary.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

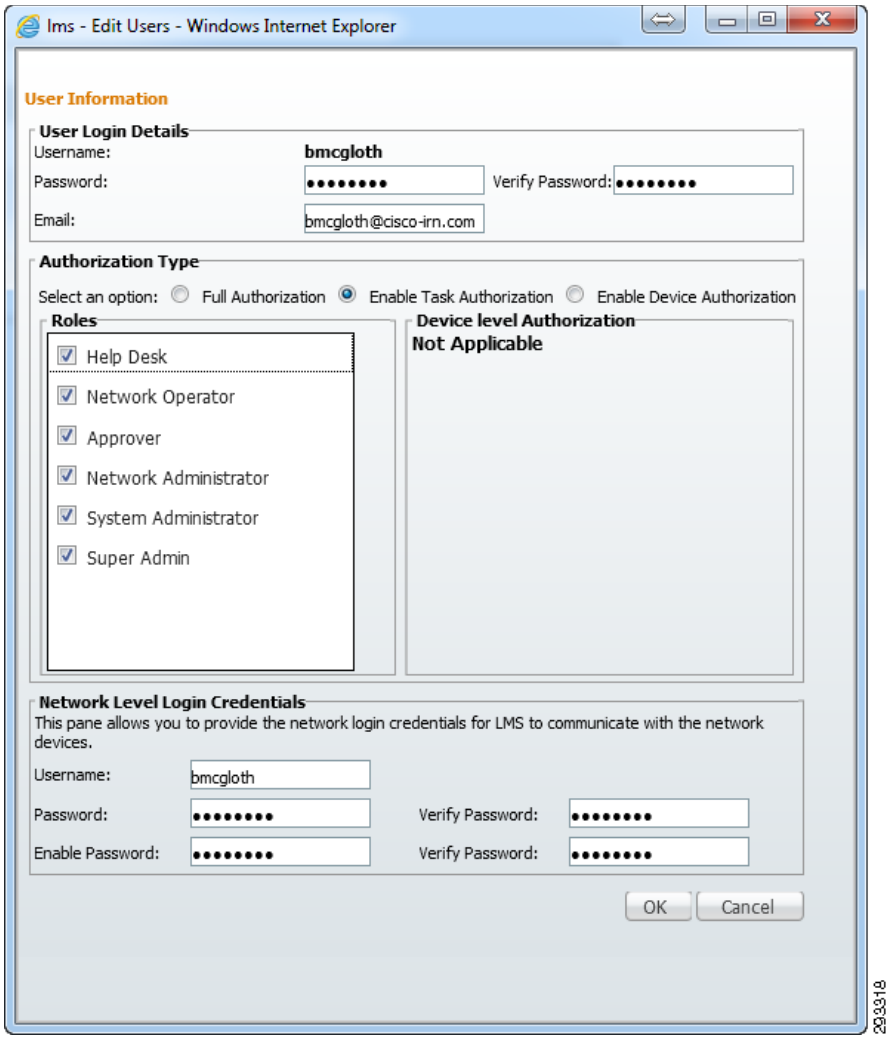
The Cisco Prime LMS is able to meet some of the requirements locally, as identified below.

- **PCI 8.1—***Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco Prime LMS supports the creation of local user accounts with unique IDs through the use of the **username** command in the CLI and via the web interface Admin > System > User Management > Local User Setup. (See Figure 5-79.) These users are necessary to role assignment and can be used for local fallback user accounts.

```
username chjanoff password hash $1$3Af9qCBs$GCZoSBOqvTIkYMLxXOeZf1 role admin
username bart password hash $1$zJe0WwVd$jHUzM9cNQxpy./D9uHCYM1 role admin
```

Figure 5-79 LMS Local User Accounts



- **PCI 8.2—***In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - Something you know, such as a password or passphrase
  - Something you have, such as a token device or smart card
  - Something you are, such as a biometric

  Local user accounts on Cisco Prime LMS require setting of a password.
- **PCI 8.4—***Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Cisco Prime LMS uses MD5-encrypted hashing of locally stored passwords.
- **PCI 8.5.5—***Remove/disable inactive user accounts at least every 90 days.*

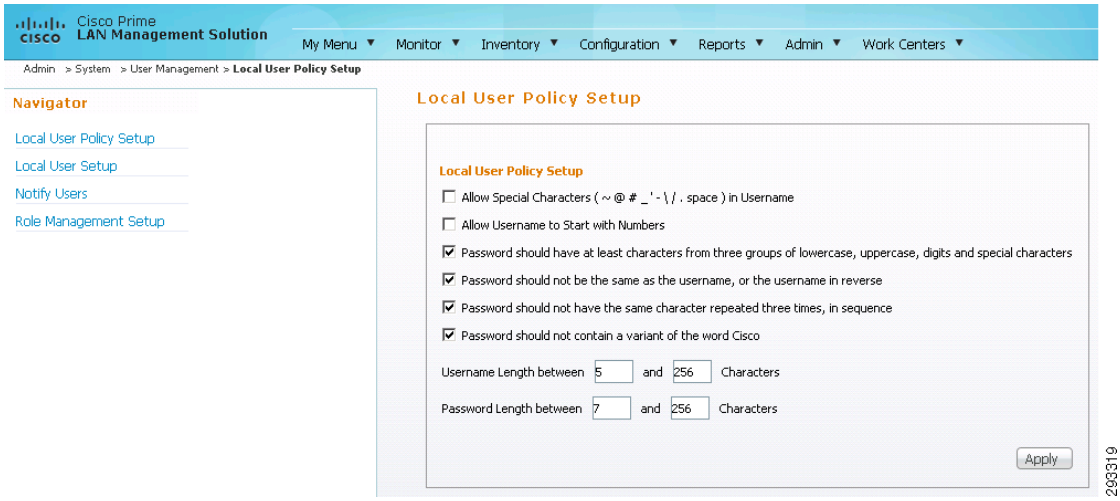
  Cisco Prime LMS does not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days.
- **PCI 8.5.9—***Change user passwords at least every 90 days.*

Cisco Prime LMS does not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Security Manager.

- **PCI 8.5.10—***Require a minimum password length of at least seven characters.*

  Cisco Prime LMS supports the ability to specify a minimum password length for local accounts in the Admin > System > User Management > Local User Policy Setup. The default minimum password length must be changed from 6 to 7 characters, as shown in Figure 5-80.

Figure 5-80 LMS Local User Policy Setup



- **PCI 8.5.11—***Use passwords containing both numeric and alphabetic characters.*

  Cisco Prime LMS supports the ability to specify the necessary password complexity for local accounts in the Admin > System > User Management >Local User Policy Setup.

- **PCI 8.5.12—***Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco Prime LMS does not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually if a centralized authentication service with this capability could not be used.

- **PCI 8.5.13—***Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco Prime LMS does not support an automated capability to perform this function at this time. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14—***Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

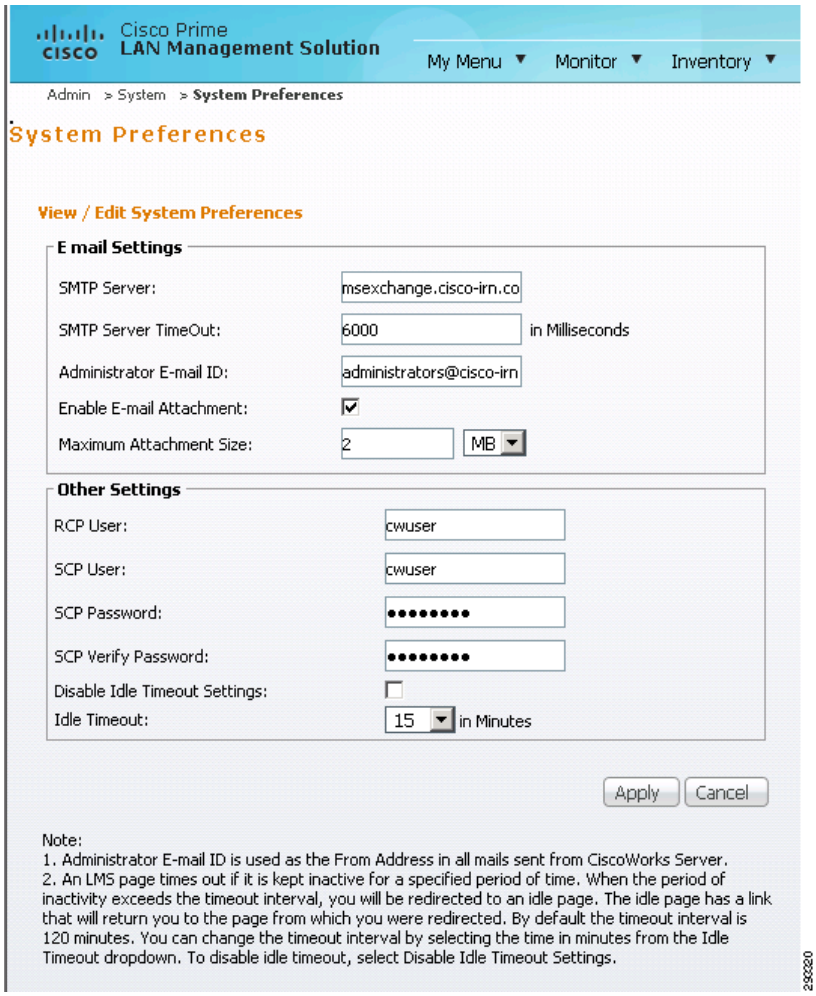
  This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15—***If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco Prime LMS management interface timeout must be properly configured to meet this requirement:

Change the Session TimeOut to 15 minutes from the default 120 minutes, as shown in Figure 5-81 on the Admin > System > System Preferences menu.

Figure 5-81 LMS System Preferences for Idle Timeout



Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Prime LMS is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*

  - **PCI 10.2.7—***Creation and deletion of system-level objects*

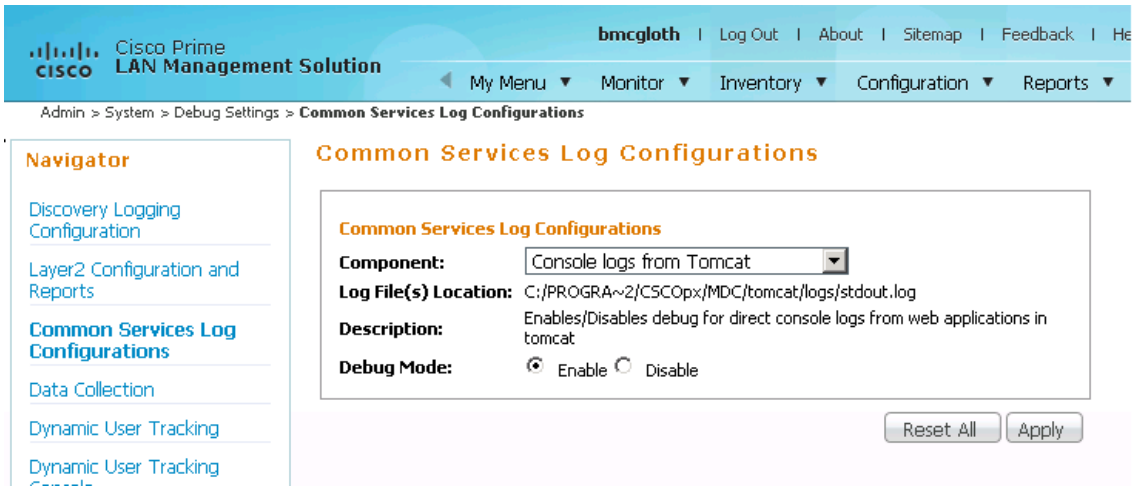
- **PCI 10.3—***Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1—***User identification*
  - **PCI 10.3.2—***Type of event*
  - **PCI 10.3.3—***Date and time*
  - **PCI 10.3.4—***Success or failure indication*
  - **PCI 10.3.5—***Origination of event*
  - **PCI 10.3.6—***Identity or name of affected data, system component, or resource.*

  The majority of LMS system activities on the server are accomplished through jobs. Each of these jobs tracks the requestor, the success or failure, the type of event, and the systems against which they are executed. The Job Browser shows status of scheduled, current and past jobs. The jobs browser is located at Admin > Jobs > Browser.

  Additional audit trail information for system configuration changes (for example, changing the authentication mode of the LMS Server from local to TACACS and back to local) require enabling debug mode logging for the Tomcat service. With debug mode enabled, the server is able to capture sufficient information for logging this configuration change and other similar system changes.

  To enable debug mode for the Tomcat console, navigate to Admin > System > Debug Settings > Common Services Log Configurations (see Figure 5-82). Select "Console logs from Tomcat" in the component dropdown. Click the **Enable** radio button and then click **Apply**.

Figure 5-82 Common Services Log Configurations



Note Enabling debugging may have a significant performance impact on the LMS system, depending on the number of users who are simultaneously accessing and managing the system. All web front end activity is logged in detail.

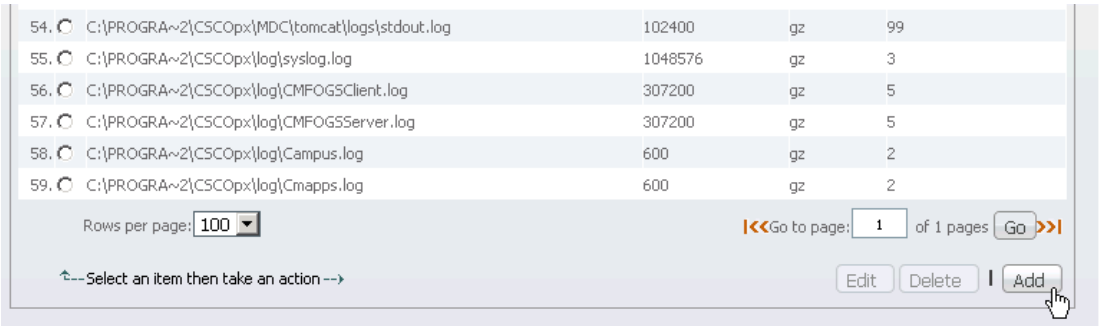
The "accesslogfilter.log" captures source IP address, date, time, and username for logged-in users as well as failed logins. Failed logins in this log have a "null" username. The attempted usernames of the failed logins appear in the Audit-Log-{date}.CSV report. These reports do not include the user's source IP address, so some manual correlation must be done between the two logs. These

reports are generated at Reports > System Audit Reports > System, or available in \CSCOpx\MDC\log\audit. Informkation about currently logged-in users is available in Reports > System > Users > Who is logged On.

The “stdout.log” and “accesslogfilter.log” files should be added to the Log Rotation under Admin > System > Log Rotation.

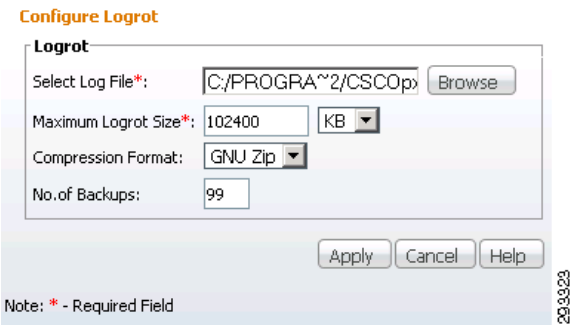
To add these logs to the rotation, click **Add** at the bottom of the page. (See Figure 5-83.)

Figure 5-83 Adding Logs to the Rotation



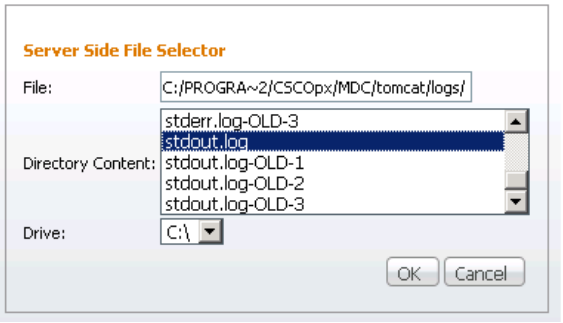
In the popup window, set the max file size needed to capture about a days’ worth of information for your environment and usage. Set the number of backups to the maximum of 99. (See Figure 5-84.)

Figure 5-84 Configure Logrot



Click **Browse** and navigate to the file location as appropriate for the operating system; for example, C:/PROGRA~2/CSCOpx/MDC/tomcat/logs/stdout.log. (See Figure 5-85.)

Figure 5-85 Server Side File Selector



Click **OK** to complete the file section, and then **Apply** to complete the addition of the log rotation file.

Cisco Prime LMS uses the local clock facilities meet the following requirements:

- **PCI 10.4.1—***Critical systems have the correct and consistent time.*
- **PCI 10.4.2—***Time data is protected.*
- **PCI 10.4.3—***Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. The Cisco Prime LMS appliance uses NTP to meet these requirements by implementing the following configuration statements:

  ```
  ntp server 192.168.62.161 192.168.62.162
  ```

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5—***Secure audit trails so they cannot be altered.*
- **PCI 10.5.1—***Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2—***Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3—***Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.4**—*Write logs for external-facing technologies onto a log server on the internal LAN.*
- **PCI 10.5.5—***Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  The Cisco Prime LMS GUI and console scripts support periodic log rotation based on file size and can be configured for the maximum size of the file and number of files to maintain. A script must be created to copy these log files off the system to an external secure repository (for example, a directory on the RSA enVision server) because LMS is not natively capable of sending system events to a centralized repository or ensuring the integrity of the logs to the standards required for PCI. This script file should be automated and scheduled to run periodically at least daily (for example, every 1, 2, or 24 hours) via the operating system (Linus, Solaris, Windows) based on the deployment OS. Logs stored locally are buffered and require operator level privileges on the system to be viewed.

Logging enabled by implementing the following configuration statements in the CLI is only for system events such as software updates via the cars application utility:

```
logging 192.168.42.124
logging loglevel 6
```

RSA enVision supports the periodic collection of log files from Cisco LMS versions 3.2 and 4.0. The old method required the daily running of a .VBS script on the server (Windows only) where a file is created in the directory/files/rme/archive directory. It then required the installation of an RSA enVision NIC SFTP Agent, which is used to transfer the log files to the RSA enVision appliance. RSA recently added support for ODBC collection of change audit information from Cisco LMS. It is highly recommended to update to the latest RSA enVision ESU and move to this ODBC method as log collection occurs more frequently. ODBC importing was not validated for LMS at the time of this publication.

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Security Manager

The Cisco Security Manager is a powerful yet easy-to-use solution for configuring firewall, VPN, and IPS policies on Cisco security appliances, firewalls, routers, and switch modules.

Cisco Security Manager helps enable enterprises to manage and scale security operations efficiently and accurately. Its end-to-end tools provide consistent policy enforcement, quick troubleshooting of security events, and summarized reports from across the security deployment.

Cisco Security Manager enables you to centrally manage security policies over 250 types and models of Cisco security devices. Cisco Security Manager supports integrated provisioning of firewall, IPS, and VPN (most site-to-site, remote access, and SSL) services across the following:

- Cisco IOS/ISR/ASR routers
- Cisco Catalyst switches
- Cisco ASA and PIX security appliances
- Cisco Catalyst Service Modules related to firewall, VPN, and IPS
- Cisco IPS appliances and various service modules for routers and ASA devices

For a complete list of devices and OS versions supported by Cisco Security Manager, see *Supported Devices and Software Versions for Cisco Security Manager* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

The high-performance and easy-to-use integrated event viewer allows you to centrally monitor events from IPS, ASA, and FWSM devices and correlate them to the related configuration policies. This helps identify problems and troubleshoot configurations. Then, using Configuration Manager, you can make adjustments to the configurations and deploy them. Event Viewer supports event management for Cisco ASA, IPS, and FWSM devices.

In addition to the Primary Event Data Store, events can be copied and stored in the Extended Event Data Store. The Extended Event Data Store can be used to back up and archive a larger number of events. This is useful for historical review and analysis of events where Event Viewer can gather event data from both the Primary Event Data Store and the Extended Event Data Store. The Extended Event Data Store can be enabled in Event Management in Security Manager's Administration settings.

For supported platforms and more information, see the "Monitoring and Diagnostics" section of the *User Guide for Cisco Security Manager 4.1* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

The new integrated report management allows you to generate and schedule ASA, IPS, and remote access VPN reports. Reports for ASA and IPS devices are created by aggregating and summarizing events collected by the Event Viewer. Security reports can be used to efficiently monitor, track, and audit network use and security problems reported by managed devices. Report Manager helps in developing and customizing reports for Cisco ASA and IPS devices.

For supported platforms and more information, see the "Monitoring and Diagnostics" part of the *User Guide for Cisco Security Manager 4.1* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

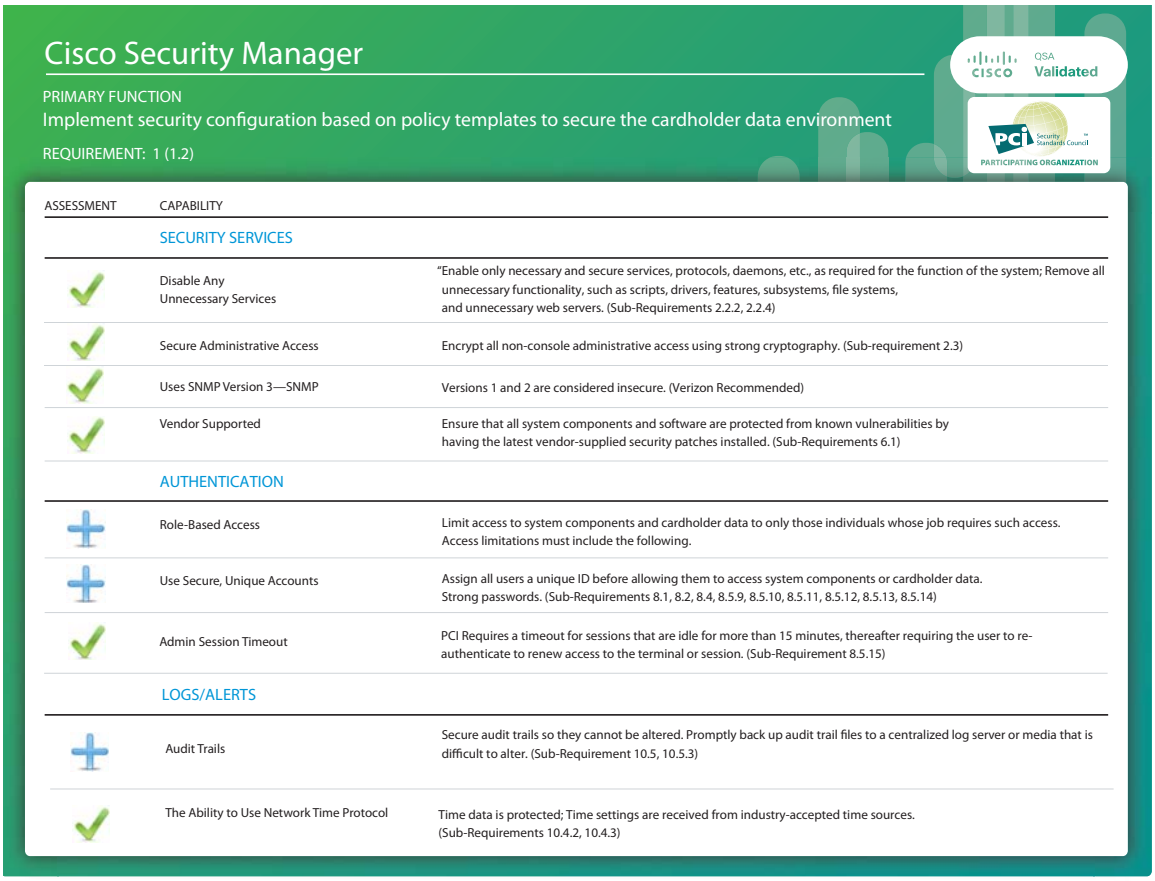
Table 5-26 PCI Assessment Summary—Cisco Security Manager

Models Assessed	
Cisco Security Manager version 4.0.1	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function of Cisco Security Manager is to implement security configuration in firewalls, routers, and intrusion detection devices based on policy templates to secure the cardholder data environment. (1.2) Table 5-27 lists the component assessment details for Cisco Security Manager.

Table 5-27 Component Capability Assessment—Cisco Security Manager



Cisco Security Manager

PRIMARY FUNCTION
Implement security configuration based on policy templates to secure the cardholder data environment

REQUIREMENT: 1 (1.2)

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Use descriptive notes for each rule set. These are displayed as remarks in the running configuration.
- Virtualize firewall rule set deployment by using a consistent interface naming standard.
- Apply the anti-spoofing feature to all interfaces using FlexConfig.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are no unnecessary services enabled by default Cisco Security Manager. Cisco Security Manager should be installed on a hardened operating system.

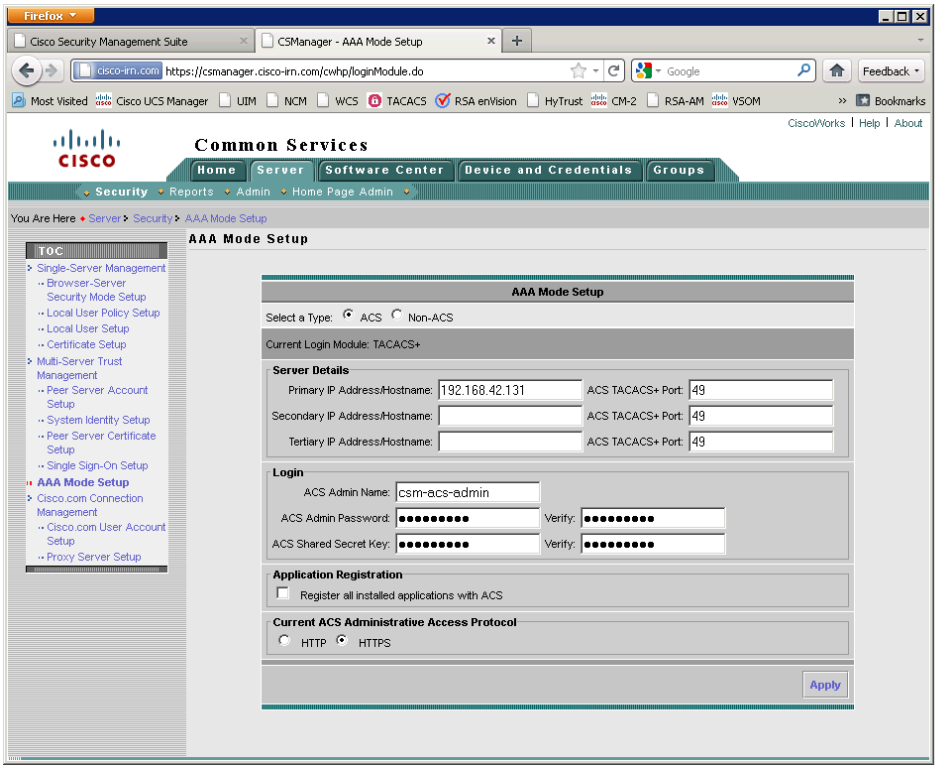
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Security Manager should be installed on a hardened operating system.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Figure 5-86 shows how the Cisco Security Manager is configured in Common Services for ensuring that only encrypted communications for administration are used.

Figure 5-86 CSM Secure Administration and AAA Policy



Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Security Manager. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Figure 5-86 shows that Cisco Security Manager AAA role setup type was implemented as Cisco Secure ACS, and identified the appropriate Cisco Secure ACS servers.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

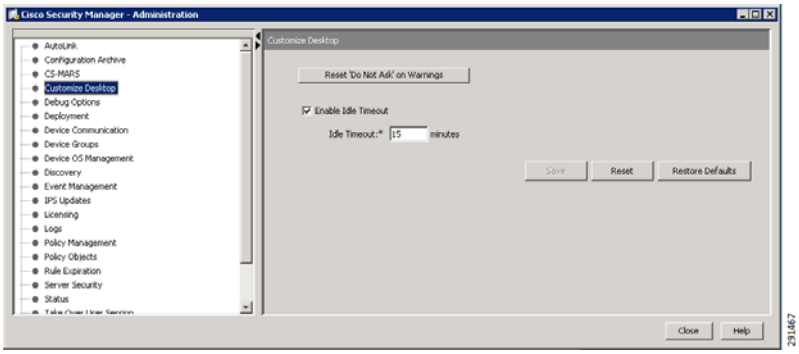
Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

Figure 5-87 shows the configuration setting in the client for setting the idle timeout.

Figure 5-87 Customize Desktop



Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Security Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Security Manager uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*

- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

Figure 5-88, Figure 5-89, and Figure 5-90 shows the Logs, Audit Report, and View Settings screens.

Figure 5-88 Logs

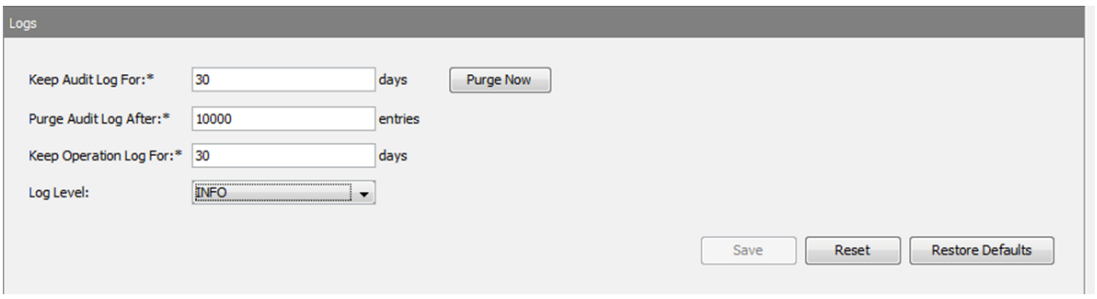


Figure 5-89 Audit Report

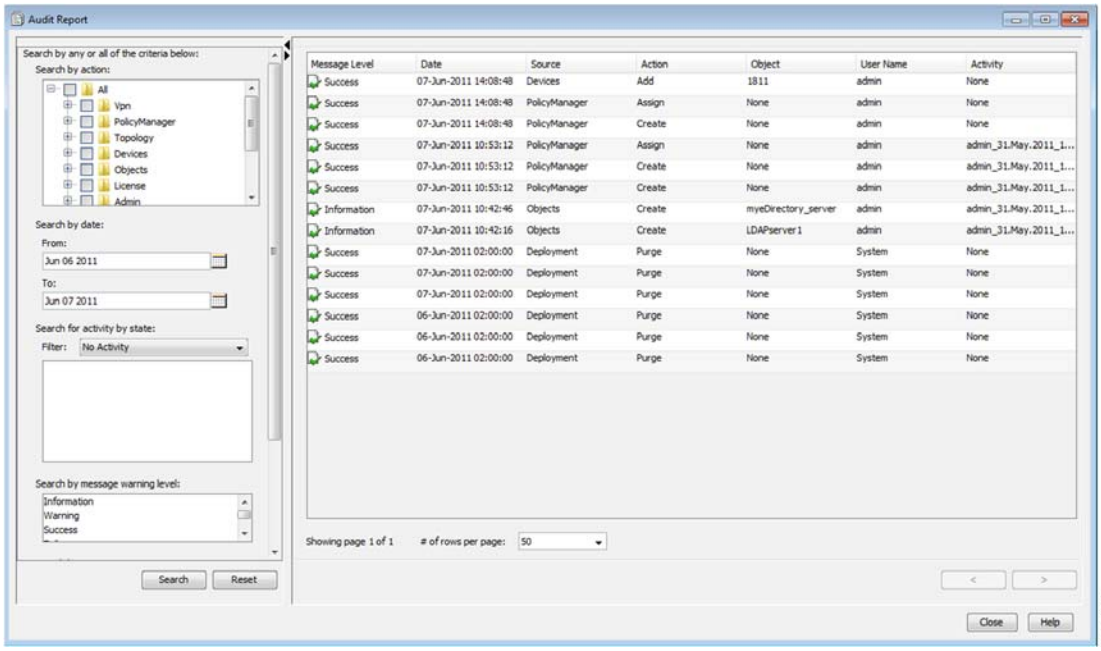
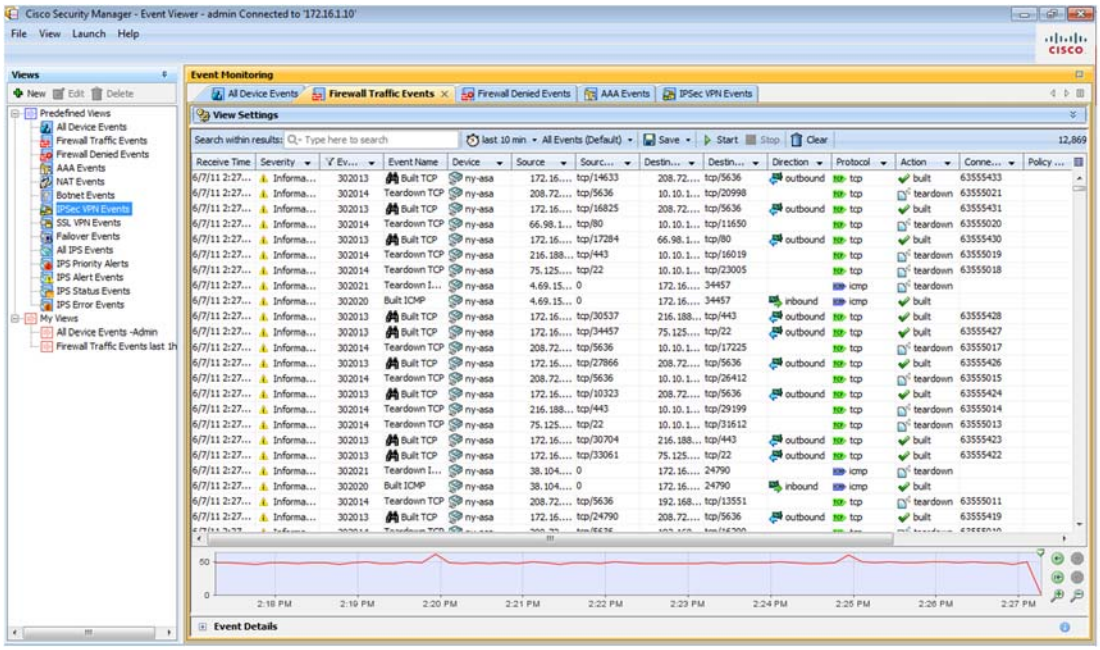


Figure 5-90 View Settings



PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

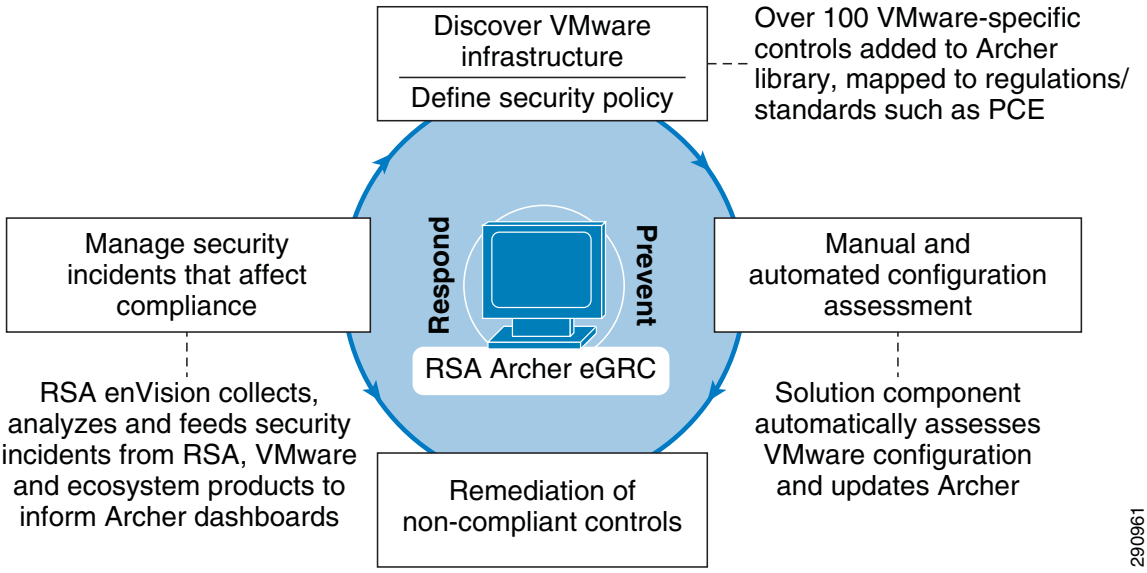
RSA Archer

The RSA Archer eGRC Suite for enterprise governance, risk, and compliance allows your organization to jumpstart your PCI compliance program by conducting continuous, automated assessments to gain the visibility you need to manage and mitigate risk.

Note RSA Archer was initially reviewed by Verizon Business and determined to be outside the scope of the PCI Audit. RSA Archer does store, process, or transmit sensitive cardholder data. There are no Assessment Summary or Capability Assessment details for this product.

RSA Archer provides a comprehensive library of policies, control standards, procedures, and assessments mapped to PCI DSS and other regulatory standards. RSA Archer is designed to orchestrate and visualize the security of both VMware virtualization infrastructure and physical infrastructure from a single console. (See Figure 5-91.)

Figure 5-91 Using Firewall and IDS/IPS



One of the major changes to PCI DSS 2.0 is its clarification on the use of virtualization technology in the cardholder data environment. If virtualization technology is used, the virtualization platform is always in scope for PCI. More than 130 control procedures in the Archer library have been written specifically for VMWare environments and have been mapped to PCI requirements. The RSA Cloud Security and Compliance solution includes software that substantially automates the assessment of whether VMware security controls have been implemented correctly. The results of these automated configuration checks are fed directly into the RSA Archer eGRC Platform, which also captures the results of configuration checks for physical assets via pre-built integration with commercially available scan technologies.

Although a significant number of the VMware control procedures are tested automatically, the remainder must be tested manually because their status cannot be directly inferred from the environment. For these control procedures, project managers can issue manual assessments from the RSA Archer eGRC

Platform, using a pre-loaded bank of questions. Project managers can create new questionnaires within minutes and issue them to appropriate users based on asset ownership. Those users are automatically notified of their assessments via rules-driven workflow and My Tasks lists, and can complete their assessments online.

Results for both automated and manual assessments are consolidated in the RSA Archer eGRC Platform and mapped to PCI DSS and other regulations and standards. IT and security operations teams can then monitor compliance with regulations and internal policies across the physical and virtual infrastructure by device, policy, procedure, regulation, and other criteria. This information is presented through a graphical dashboard view, making the information easy to digest and understand.

Configuring the physical and virtual infrastructure according to best-practice security guidelines and regulatory requirements is critical. However, the security and compliance process does not stop there. Organizations also require the ability to monitor misconfigurations, policy violations, and control failures across their infrastructure; and to respond swiftly with appropriate remediation steps. Deficiencies identified through automated and manual configuration checks are captured within the RSA Archer eGRC Platform for management. Control failures are then assigned to appropriate personnel, who can respond by completing remediation tasks or logging exception requests that identify effective compensating controls and are tracked in a Policy Management dashboard, as shown in Figure 5-92.

Figure 5-92 RSA Archer Policy Management



Encryption

A subtle, yet potentially significant change to key management has been introduced with the PCI 2.0 standard. With past versions of the DSS, annual key rotations were required for encryption keys. PCI DSS 2.0 now requires that keys are rotated at the end of their *cryptoperiod*, and references the NIST 800-57 Special Publication to determine what an appropriate cryptoperiod is. The NIST 800-57 Special

Publication is a 324-page, three-part document. Organizations, and even QSAs, may not have the expertise to fully understand such a document that includes countless encryption scenarios, with cryptoperiods ranging from as short as a day and as long as three years.

In an ideal world, with all parties being expert cryptographers, this risk-based change to the standard would be very appropriate and most welcome. However, given the number of scenarios and criteria for determining an appropriate cryptoperiod, it could suggest that this change is too subjective and may become a point of contention between an organization and QSA assessor, as to what is an appropriate cryptoperiod, whereas the former, more prescriptive control, did not allow for flexibility in this area.

RSA Data Protection Manager

RSA Data Protection Manager (formerly RSA Key Manager) provides encryption, tokenization, and key management capabilities. It can be used to achieve PCI Requirement 3 compliance for protecting stored cardholder data, regardless of where the information resides.

RSA Data Protection Manager is an easy-to-use management tool for encrypting keys at the database, file server, and storage layers. It is designed to lower the total cost of ownership and simplify the deployment of encryption throughout the enterprise. It also helps ensure that information is properly secured and fully accessible when needed at any point in its lifecycle through a powerful management console and built-in high availability features. RSA Data Protection Manager provides a comprehensive platform for enforcing and managing the security of sensitive data.

Table 5-28 PCI Assessment Summary—RSA Data Protection Manager

Models Assessed	
RSA Data Protection Manager	version KM-3.1 / AM-6.1.SP3
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of RSA Data Protection Manager is to securely manage the keys that protect cardholder data. (3.5)

Table 5-29 lists the component assessment details for RSA Data Protection Manager.

Table 5-29 Component Capability Assessment—RSA Data Protection Manager

RSA Data Protection Manager

PRIMARY FUNCTION
Securely manage the keys that protect cardholder data

REQUIREMENT: 3 (3.5)

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
✓	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
✓	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

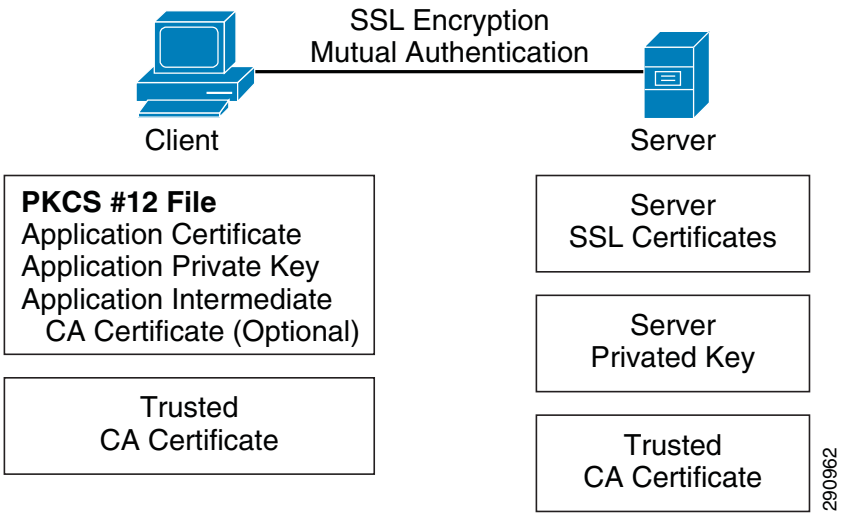
RSA Data Protection Manager's encryption and key management capabilities can be used to store the data in a compliant manner. RSA Data Protection Manager provides application development libraries that support a wide range of development languages and enables developers to easily integrate encryption into point-of-sale, payment, CRM, ERP, and other business applications that create or process sensitive information. RSA Data Protection Manager can also be used to encrypt data as it flows to both disk and tape by providing key management services to Cisco MDS or EMC storage systems.

Because there were no card handling applications in the simulated lab environment, RSA Data Protection Manager was integrated with Cisco MDS to encrypt all data in the environment regardless of whether it was cardholder data or not.

Public Key Infrastructure (PKI) Requirements

In an RSA Data Protection Manager deployment, a PKI needs to be set up to enable secure communication between the RSA Data Protection server and its clients. (See Figure 5-93.)

Figure 5-93 RSA Data Protection Manager Deployment



The certificates and credentials that need to be prepared include:

- Client PKCS#12 certificate and key pair—Used to authenticate RSA Data Protection Manager clients to the RSA Data Protection Server
- Server SSL certificate and key pair—Used by RSA Data Protection Manager Clients to authenticate the server
- Trusted CA certificate—Installed on both clients and the server to verify the signature of certificates sent by a peer. For example, a RSA Key Manager Client has a trusted CA certificate to verify the signature of the Server certificate.
- Middle CA certificate (optional)—If a certificate is not signed directly by a trusted CA certificate, a middle CA certificate should be installed and sent during SSL connection to verify the certificate chain.

Security Recommendation

Because of vulnerabilities with RSA signatures with a small public exponent, especially 3, RSA recommends that an exponent of F4 (216+1) be used.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The appliance version of RSA Data Protection Manager comes pre-hardened. The software version must be installed into a hardened operating system, application server, and database server.

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The appliance version of RSA Data Protection Manager comes pre-hardened. The software version must be installed into a hardened operating system, application server, and database server.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  RSA Data Protection Manager administrative interfaces are protected using SSL.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  RSA Data Protection Manager publishes security patches at RSA Secure Care Online (https://knowledge.rsasecurity.com/) in accordance with industry best practices to manage and respond to security vulnerabilities to minimize customers' risk of exposure.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the included RSA Access Manager Internal Database. Within RSA Data Protection Manager (and the included Access Manager), individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

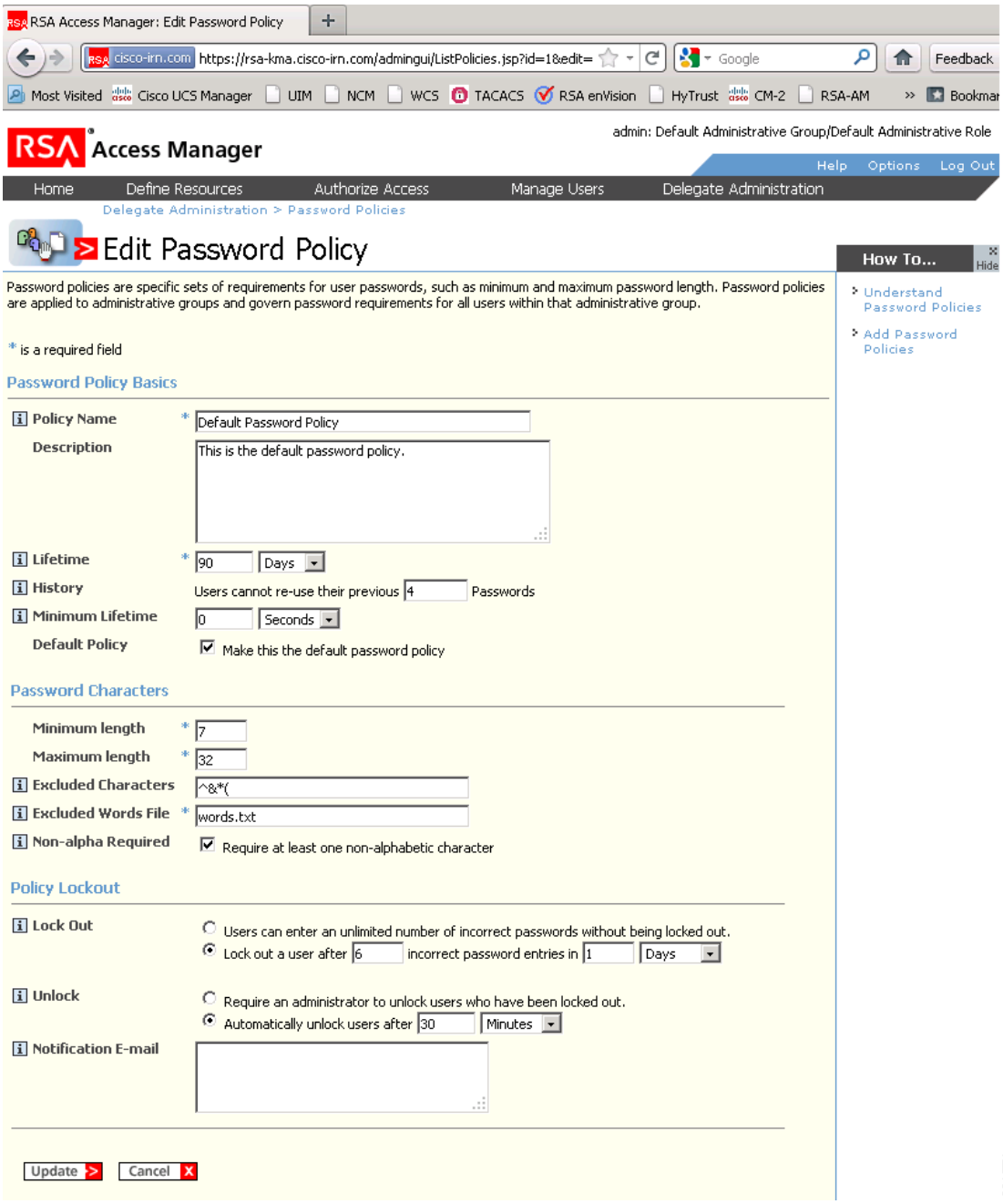
- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  RSA Data Protection Manager embeds and is protected by RSA Access Manager, which has very powerful and flexible capabilities to define password and account lockout policies that can meet all of the above criteria.

  Configuration of user policies is performed via the administration console that can be accessed at the following URL: https://<server address>/admingui/Login.jsp.

  Figure 5-94 shows an appropriate password policy for PCI compliance.

Figure 5-94 Password Policy Settings



Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database, as shown below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  RSA Data Protection Manager supports the creation of local users. Through company policy, each user must be assigned a unique ID.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts in RSA Data Protection Manager require the setting of a password according to the assigned password policy
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Through company policy, inactive users should be removed or disabled every 90 days. RSA Data Protection Manager also enables setting of an account expiration date for individual accounts.
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  The Default Password policy can be configured to force users to change their passwords every 90 days, as shown in Figure 5-94.
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The Default Password policy can be configured to require a minimum of 7 characters, as shown in Figure 5-94.
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The Default Password policy can be configured require at least one non-alphabetic character by checking the "Non-Alpha Required" box, as shown in Figure 5-94.
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The Default Password policy can be configured to prevent the re-use of previous passwords by specifying the history number, as shown in Figure 5-94.
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  The Default Password policy can be configured to lock out accounts after a specified number of login failures, as shown in Figure 5-94.
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  The Default Password policy can be configured to lock out accounts for a specified duration or until the administrator re-enables the user ID, as shown in Figure 5-94.
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  RSA Data Protection Manager automatically closes sessions to the administrative consoles after 15 minutes of inactivity.

  RSA Data Protection Manager embeds and is protected by RSA Access Manager, which has very powerful and flexible capabilities to define password and account lockout policies that can meet all of the above criteria.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

RSA Data Protection Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

RSA Data Protection Manager uses Network Time Protocol (NTP) to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. The appliance uses NTP to meet these requirements by specifying the appropriate NTP servers during the installation steps. If NTP servers need to be modified, use the following steps:

  1. Open the /etc/ntp.conf file.
  2. Under the List Servers section, provide the ntp server ip address or host name to the server parameter.
  3. Save the /etc/ntp.conf file.
  4. Execute the following commands (as root) to forcibly synchronize the clock of the appliance to the NTP server:

  a. Stop the NTPD daemon by typing the following:

  ```
  service ntpd stop
  ```

  b. Execute the following command at least three times (to minimize the offset):

  ```
  ntpdate -u <ntpserver>
  ```

  c. Start the NTPD daemon by typing the following:

  ```
  service ntpd start
  ```

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*

  Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  RSA Data Protection Manager can be configured to send its log data to the RSA enVision log management platform to meet the above requirements. The configuration procedure is documented in the enVision Event Source Configuration Guide for RSA Data Protection Manager, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/)

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Storage

EMC SAN Disk Array

The EMC SAN disk array is used to securely store sensitive compliance data within the data center. Using virtual storage technology, organizations are able to safely combine (in-scope) sensitive date with (out-of-scope) data while maintaining the compliance boundary.

EMC technology combines midrange networked storage with innovative technology and robust software capabilities to manage and consolidate your data.

Table 5-30 PCI Assessment Summary—EMC SAN Disk Array

Models Assessed	
EMC CLARiiON CX-240 EMC Unified Infrastructure Manager version 2.0.1.1.160	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15

Table 5-30 PCI Assessment Summary—EMC SAN Disk Array (continued)

PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of the EMC SAN disk array is to store cardholder data. There is no direct PCI requirement for this storage function.

Table 5-31 lists the component assessment details for the EMC SAN disk array.

Table 5-31 Component Capability Assessment—EMC SAN Disk Array

EMC SAN Disk Array

PRIMARY FUNCTION
Securely manage the keys that protect cardholder data

REQUIREMENT: 3 (3.5)

cisco QSA Validated

PCI Security Standards Council PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

The EMC SAN disk array is a primary component of VCE Vblock architecture. Vblock 1 is designed for medium-to-high numbers of virtual machines, and is ideally suited to a broad range of usage scenarios, including shared services, e-mail, file and print, virtual desktops, and collaboration.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The storage management server provides 256-bit symmetric encryption of all data passed between it and the client components that communicate with it, as listed in the "Port Usage" section (Web browser, Secure CLI), as well as all data passed between storage management servers. The encryption is provided via SSL/TLS and uses the RSA encryption algorithm
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The EMC Storage system does not run any unnecessary services by default.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  When you connect to Unisphere through http://<clariion_ip> (port 80), a Java applet is delivered to the browser on your computer. The applet establishes a secure connection over SSL/TLS (port 443) with the storage management server on the CLARiiON storage system. Therefore, even though "https://" is not displayed in the browser, the connection is secure.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  EMC Powerlink services provide ongoing access to software updates and security patches.

  CLARiiON storage systems do not support installation of third-party utilities or patches. EMC will provide an officially released FLARE Operating Environment patch if needed to correct a security-related issue (or any other kind of issue).

  For information on product updates, see the following URL:
  https://support.emc.com/products/CLARiiONCX4

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by the EMC SAN disk array using LDAP services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

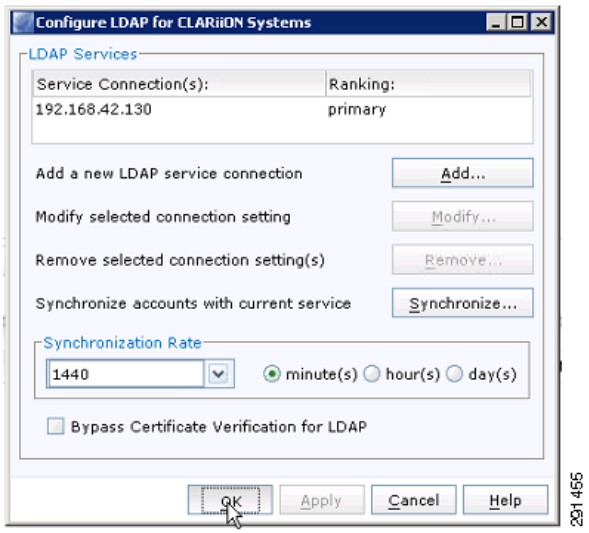
When you start a session, Unisphere prompts you for a username, password, and scope (local, global, or LDAP). These credentials are encrypted and sent to the storage management server. The storage management server then attempts to find a match within the user account information. If a match is found, you are identified as an authenticated user.

LDAP Authentication should be used for PCI compliance because the local authentication does not meet all PCI 8 requirements for secure user access and accounts.

Step 1 To configure LDAP authentication, go to the Domains tab, then select **Configure LDAP for CLARiiON Systems** from the Users menu on the left.

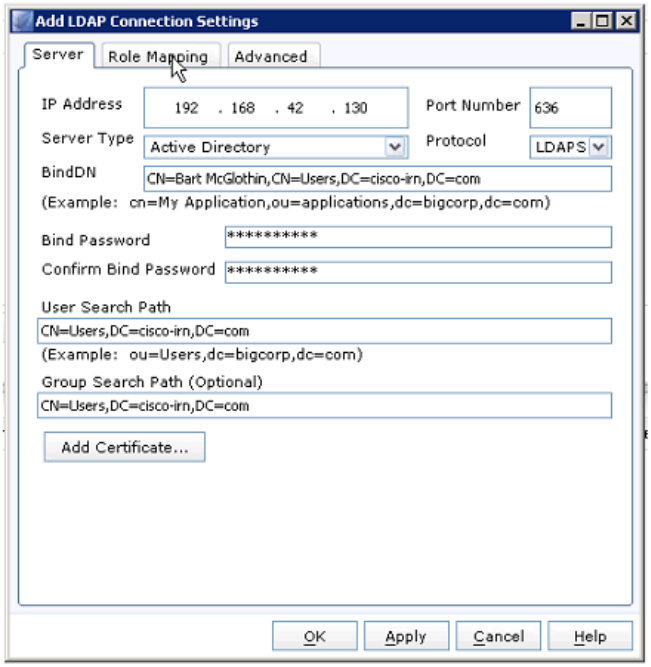
Step 2 Add a new LDAP service by clicking **Add** and then **OK**, as shown in Figure 5-95.

Figure 5-95 Adding LDAP Service



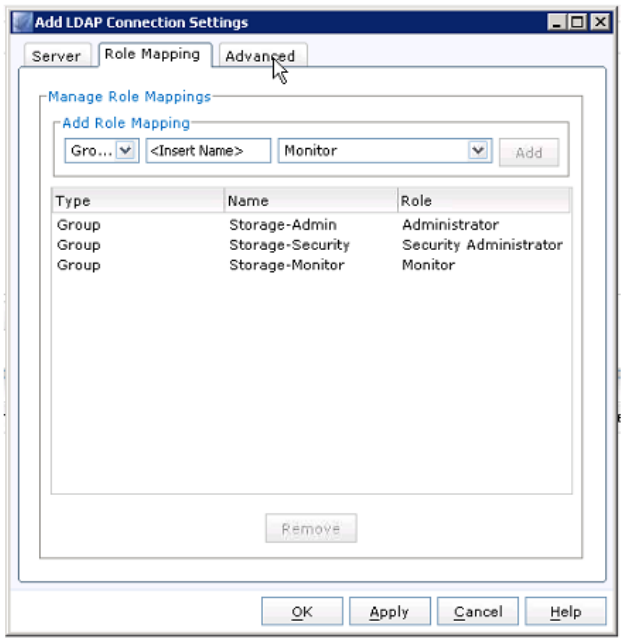
Step 3 Configure the LDAP server for Active Directory as shown in Figure 5-96.

Figure 5-96 Configuring the LDAP Server for Active Directory



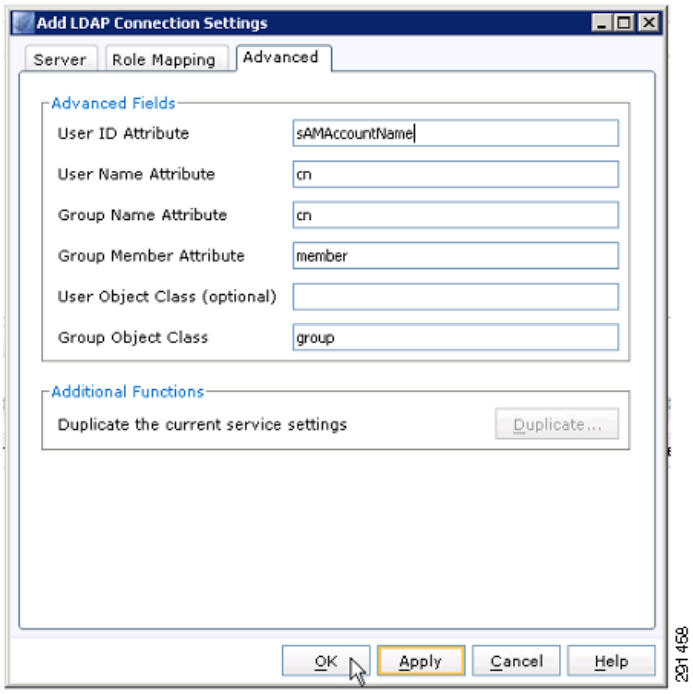
Step 4 After communications are established with the LDAP service, specific LDAP users or groups must be given access to Unisphere by mapping them to Unisphere roles. The LDAP service merely performs the authentication. Once authenticated, user authorization is determined by the assigned Unisphere role. The most flexible configuration is to create LDAP groups that correspond to Unisphere roles. This allows you to control access to Unisphere by managing the members of the LDAP groups. Roles were configured as shown in Figure 5-97.

Figure 5-97 Role Mapping



Step 5 The Advanced features were left at their default settings, as shown in Figure 5-98.

Figure 5-98 Advanced Settings



Step 6 You can then log out, and log back in, selecting the **Use LDAP** option for centralized authentication, as shown in Figure 5-99.

Figure 5-99 Selecting Use LDAP Function



Step 7 For further installation information, see the *FLARE 30 Security Configuration Guide* on EMC Powerlink for configuring LDAP/Active Directory authentication.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the LDAP authentication capabilities to the Windows Active Directory server for AAA services. Microsoft Active Directory contains the necessary user account services for all of the appropriate PCI 8 requirements. Configure AAA services as shown above in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.PCI Sub-Requirements with Compensating Controls*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

EMC CLARiiON is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*

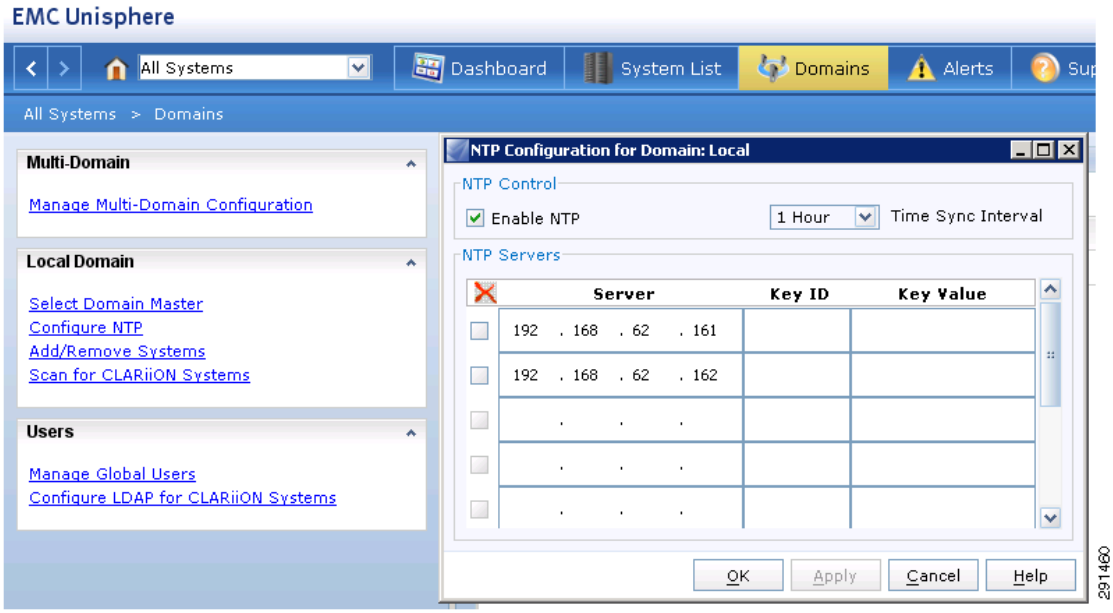
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

EMC CLARiiON uses Network Time Protocol (NTP) to update and synchronize local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. EMC CLARiion uses NTP to meet these requirements by implementing the configuration statements shown in Figure 5-100.

Figure 5-100 NTP Configuration for Domain: Local



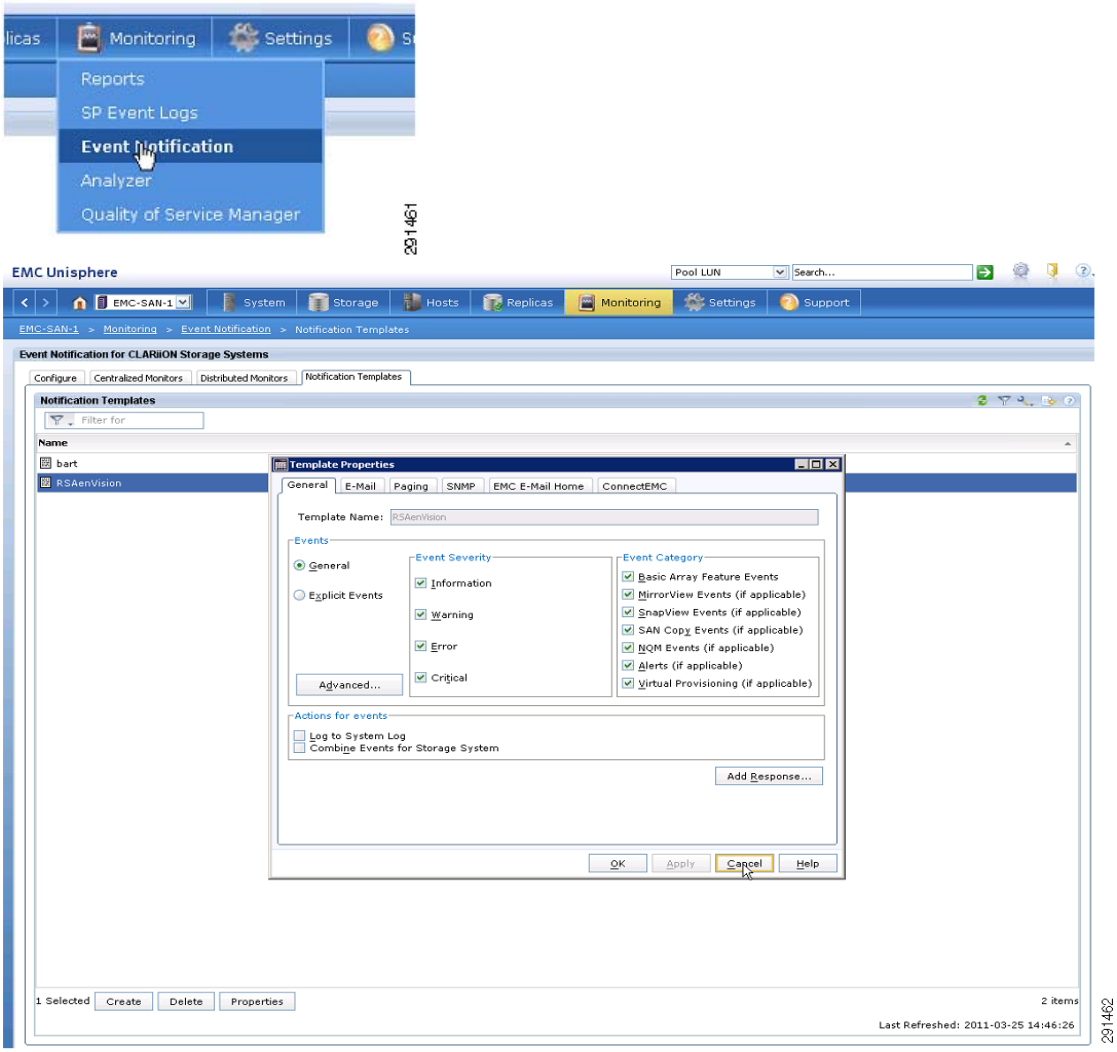
- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

  PCI 10.5.5—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

SP event logs on CLARiiON storage systems can store only a fixed number of events and will wrap if that limit is exceeded. This may take days, weeks, months, or years depending on the logging activity. Therefore, because PCI requires keeping all logs for a set period of time, you need to archive the logs from the CLARiiON storage system on a regular basis. You can do this with the CLI **getlog** command, but a much more integrated method is to use the "log to system log" option of the Event Monitor template to log events to the Windows system log. You can then archive these logs as required.

Additional SNMP Traps are configured to send event notifications directly and immediately to RSA enVision. (See Figure 5-101.)

Figure 5-101 Using Log to System Log Option



PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls—EMC SAN

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Monitoring

RSA enVision

RSA enVision is a security information and event management (SIEM) platform that provides the capability to implement PCI requirement 10 to track and monitor all access to network resources and cardholder data. RSA enVision does this by collecting, permanently archiving, and processing all the log and event data generated by devices and applications within your network, and generating alerts when it observes suspicious patterns of behavior. Administrators can interrogate the full volume of stored data through an intuitive dashboard, and can use advanced analytical software to gain visibility and understanding of how their network is used and the threats and risks to the infrastructure and applications.

The RSA enVision platform can draw logs from tens of thousands of devices at once, including Cisco network devices, the VCE Vblock infrastructure, the VMware virtual environment, Cisco ASA firewalls, Cisco IPS devices, Cisco IronPort E-mail Appliance, other RSA products, and the HyTrust appliance. Out of the box, RSA enVision can produce PCI 2.0 compliance reports and alerts based on the log and event data it collects. RSA enVision also offers powerful tools to create custom reports and alerts specific to your environment.

Table 5-32 PCI Assessment Summary—RSA enVision

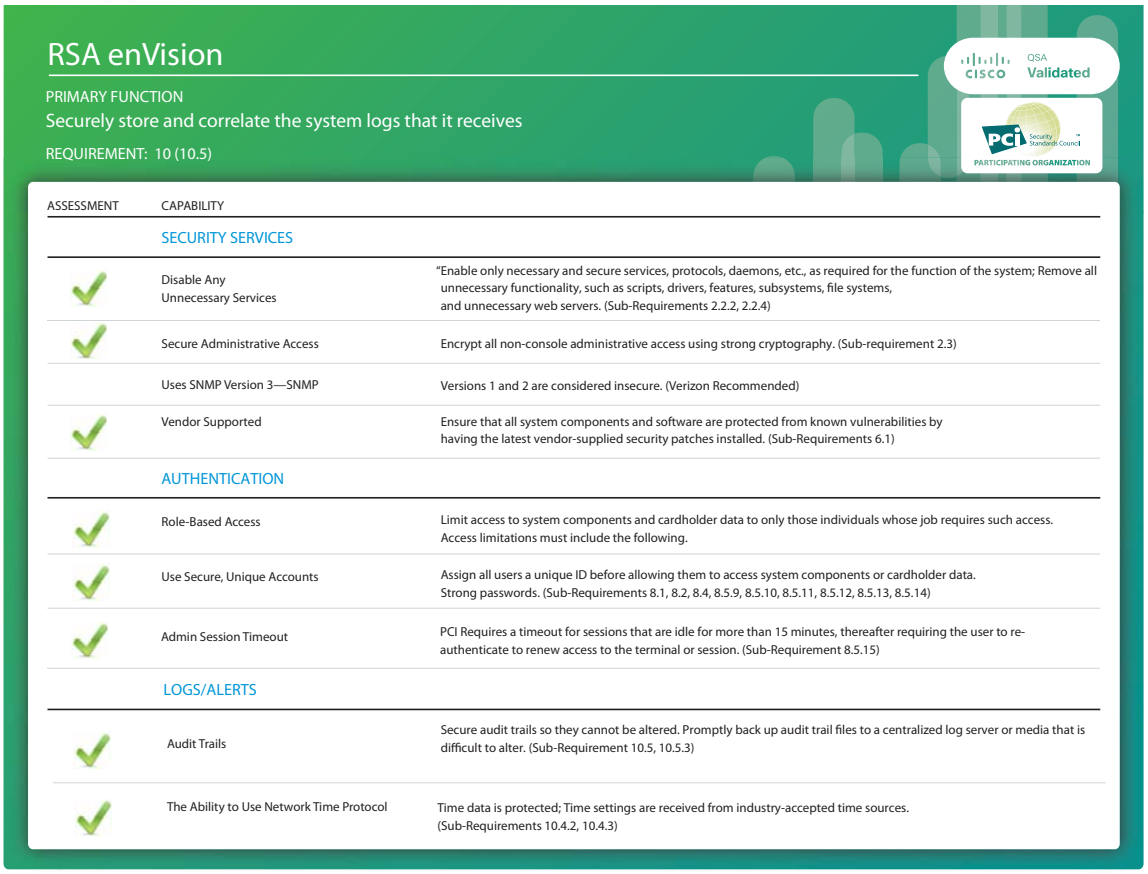
Models Assessed	
RSA enVision version 4.0, Revision 5	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of RSA enVision is to securely store and correlate the system logs that is receives. (10.5)

Table 5-33 lists the component assessment details for RSA enVision.

Table 5-33 Component Capability Assessment—RSA enVision



RSA enVision

PRIMARY FUNCTION
Securely store and correlate the system logs that it receives

REQUIREMENT: 10 (10.5)

QSA Validated

PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
✓	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
✓	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
✓	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

Depending on the size of your network, RSA enVision may be deployed as a standalone, self-contained, security-hardened appliance or in a distributed deployment to cope with the demands of the largest enterprise networks. When deployed in a distributed architecture, multiple dedicated appliances are deployed where required to perform key roles. Local and remote collectors perform data collection. Data servers manage the data. Application servers perform analysis and reporting. Data itself can be stored using direct attached, online, near-line or offline storage from the full EMC storage portfolio.

RSA enVision does not require any client-side agents to pull log or event data from your infrastructure or applications. RSA enVision can integrate with event sources through standard protocols such as syslog or SNMP by configuring the event source to send data to enVision. For richer event data, enVision integrates with some event sources through their APIs or directly with their database backends. Specific event source device configuration procedures can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/)

RSA enVision is sold as a standalone appliance. It is available in a variety of hardware options based on the requirements of the enterprise design. The system comes pre-installed on an already hardened operation system.

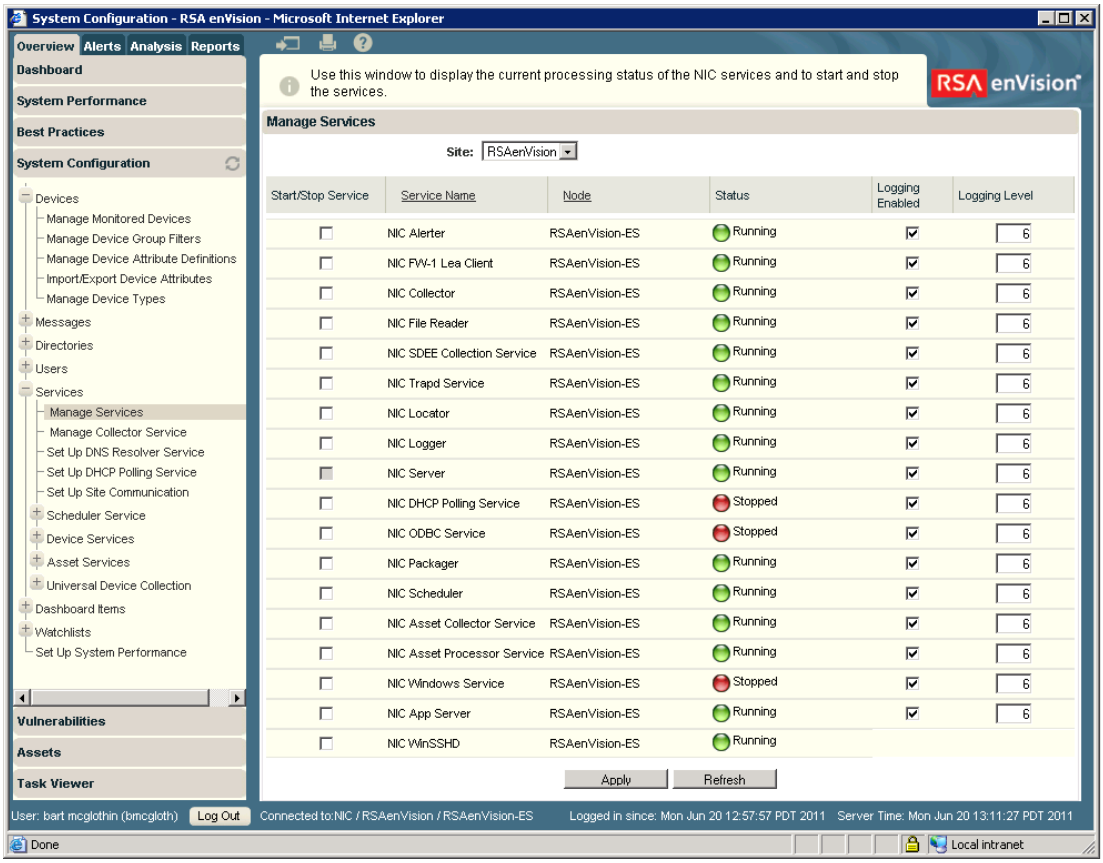
PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  RSA enVision services can be independently enabled or disabled, depending on what protocols are required to collect log and event data, as shown in Figure 5-102.

Figure 5-102 RSA enVision Managed Services



- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The RSA enVision appliance ships security-hardened. The embedded Windows 2003 server is hardened to remove all unnecessary functionality.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The RSA enVision web interface is protected using SSL.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  RSA enVision publishes security patches on RSA Secure Care Online (https://knowledge.rsasecurity.com/) in accordance with industry best practices to manage and respond to security vulnerabilities to minimize customers' risk of exposure.

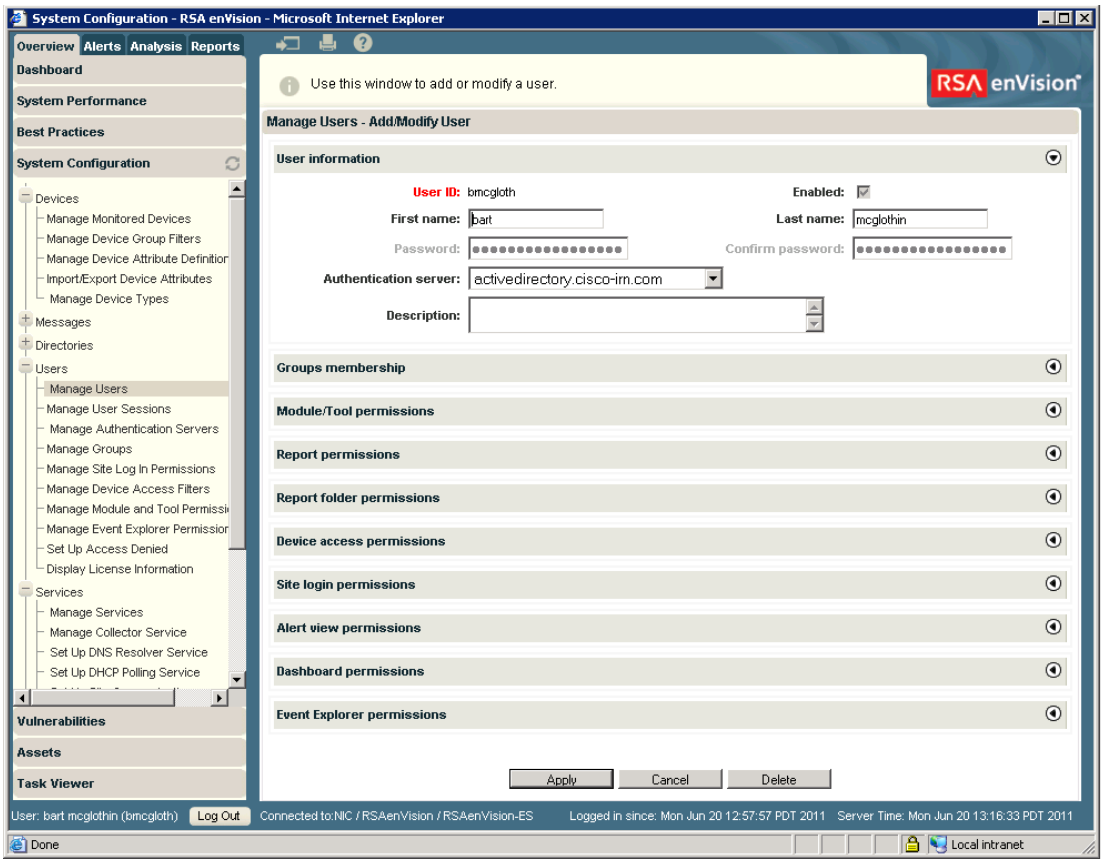
Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 can be met using the RSA enVision Internal Database (as part of its local Windows Active Directory). For validation, RSA enVision was linked to the centralized user database (Active Directory) using LDAP. Within RSA enVision, individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

RSA enVision management interfaces implement role-based access control that can be used to restrict access to privileged user IDs, as shown in Figure 5-103.

Figure 5-103 RSA enVision User Profile

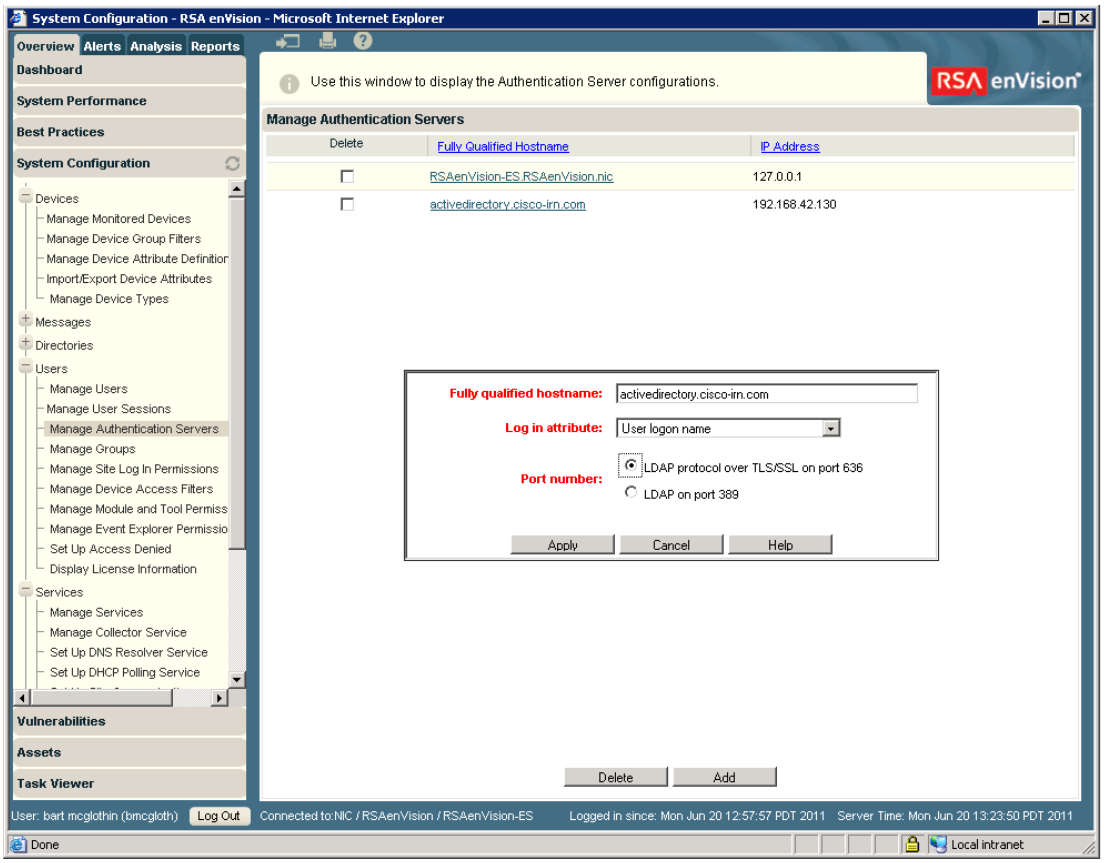


- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

RSA enVision's access control system defaults to deny access.

RSA enVision is configurable to use its local Active Directory database, or an external database via LDAP, as shown in Figure 5-104.

Figure 5-104 RSA enVision Authentication Servers



Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the LDAP authentication capabilities to the Windows Active Directory server for AAA services. Microsoft Active Directory contains the necessary user account services for all of the appropriate PCI 8 requirements. Configure AAA services as shown above in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  RSA enVision can authenticate users against external authentication services such as Windows Active Directory using the LDAP protocol. The above policies can be implemented within Windows Active Directory as was validated in this solution.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

RSA enVision is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

RSA enVision uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4**—*Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for this windows server is specified through the Domain Policy because the RSA enVision appliance is itself a Domain Controller. The server synchronizes its clock to know time sources using NTP as specified in the initial appliance setup. This synchronization allows

events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*

  Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

  RSA enVision delivers mirrored, unfiltered data to its Internet Protocol Database, which provides the ability to retain data in its original format. Further, "write once, read many" capabilities help ensure that the mirrored copy remains intact, even if the original data is compromised. RSA enVision-captured event logs are stored on a hardened operating system and protected using an integrity check mechanism.

- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*

  RSA enVision's management interfaces implement a role-based access control system to limit who has access to log data.

- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*

  RSA enVision-captured event logs are stored on a hardened operating system in a compressed form and protected via an integrity check mechanism. Access to the operating system and enVision management interfaces can be restricted through operating system and enVision access control systems.

- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

  RSA enVision's primary function is to provide a centralized point for tracking and monitoring access to cardholder data throughout a PCI environment.

- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  RSA enVision stores event data in a tamper evident manner using an internal integrity checking mechanism.

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

HyTrust Appliance

Vblock Infrastructure Platforms from VCE allow organizations to take advantage of the architectural, operational, and financial benefits of virtualization in their PCI infrastructure. HyTrust Appliance (HTA) complements Vblock capabilities by providing:

- Access control for virtual infrastructure including least privilege, separation of duties, and two-factor authentication
- Granular and exhaustive logging and auditing
- Segmentation of infrastructure to support virtualized applications

PCI DSS 2.0 clarifies the use of virtualization technology with the cardholder data environment (CDE) and specifies that the platform is always in scope. This requirement is consistent with additional risks introduced by mobility and the fast-paced change rate of virtualized assets that can now be reconfigured, relocated, and duplicated by remote administrators. These capabilities combined with poor access control create a significant risk. Hypervisor logs geared toward software maintenance and troubleshooting are obviously useful, but not in the context of a compliance audit.

HyTrust Appliance systematically addresses the three broad areas of IT control objectives (access and user administration, change and configuration, and operations), by proactively enforcing policies for all administrative access, regardless of access method: Secure Shell (SSH) to host, VMware vSphere client to host, or VMware vCenter or any of the programmatic access. HyTrust Appliance provides two-factor authentication and role-based access control, logical segmentation of shared infrastructure, root password vaulting, and audit-quality logs of every attempted access.

Table 5-34 PCI Assessment Summary—HyTrust Appliance

Models Assessed	
HyTrust version 2.2.1.14064	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function of HyTrust Appliance is to provide an automated control and audit facility for the virtual infrastructure and cloud stack. (2, 7, and 10).

Table 5-35 lists the component assessment details for the HyTrust Appliance.

Table 5-35 Component Capability Assessment—HyTrust Appliance

HyTrust Appliance

PRIMARY FUNCTION

Monitor and secure access to the virtual infrastructure by proxying administrative sessions to VMware vCenter

REQUIREMENT: 2, 7, 10 (2.3, 7.1, 10.5)

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

Define rules and deploy policy to activate protection for the virtual infrastructure.

Administrators can define custom rules that restrict entitlement based on specific virtual infrastructure objects that users need to access and manage. Rules that define entitlement can be based on pre-defined roles or administrators can use custom user-defined roles.

The Hytrust appliance provides complete logging of administrator actions by proxying VMware vCenter client connections to the vSphere management server, and clients that try to connect directly to ESX/ESXi hosts. This logging includes the source IP address of the clients, permitted actions and actions that are blocked because the client may not have sufficient privileges (all requirements of PCI that VMware cannot perform natively).

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  HyTrust Appliance configures the virtualization platform (VMware ESX server) to disable unsecure protocols. In addition, HyTrust Appliance proxies non-console management access and redirects attempts to connect via the HTTP management protocol to HTTPS-based connections. In the reference implementation, the configuration of VMware ESX 4.0 servers was performed in accordance with the HyTrust default PCI configuration template. Specifically, the following controls are set:

```
ssh_config: Protocol = 2
sshd_config:
Protocol = 2
X11Forwarding = yes
IgnoreRhosts = yes
RhostsAuthentication = no
RhostsRSAAuthentication = no
HostbasedAuthentication =no
PermitRootLogin = no
PermitEmptyPasswords = no
Banner = /etc/issue.net if not set
```

  Check that a BIOS password is set and that it is not the manufacturer default. For more information, see the following URL: http://www.pwcrack.com/bios.shtml

  Set file permissions on */etc/snmp.conf* and */etc/snmp.conf/preesx* to 700, and set *root* as owner and group.

  Replace the default “COMMUNITY” phrase with a stronger passphrase.

  Restrict SNMP access to authorized IP addresses on a separate admin-network.

  Use read-only mode.

```
- chown root:root & chmod 0600 /etc/security/console.perms or
/etc/security/console.perms.d/50-default.perms
- comment out the lines as needed
- chmod 644 /etc/{profile, pam.d/system_auth, ntp.conf, passwd, group}
- chmod 600 /etc/ssh/sshd_config
- chmod 755 /etc/{ntp, vmware}
- chmod 440 /etc/sudoers
- chmod 400 /etc/shadow
```

  Establish the following local firewall settings:

```
Ports: 22/sshd/inTCP, 53/dns/outUDP, 67-68/dhcp/UDP, 80/http/inTCP, 427/cim slp/TCP,
443/https/inTCP, 902/vmwareauthd/ inTCP-outTCPUDP, 2050-5000/vmware/TCPUDP,
5988-89/cim server/inTCP, 27000/license server/outTCP
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  HyTrust Appliance configures the virtualization platform (VMware ESX server) to disable unnecessary boot services. In addition, HyTrust Appliance restricts the use of **sudo** and **su** services and ensures tighter configuration of copy and paste sharing between the host hypervisor and CDE implemented as a virtual system component.

  In addition, HyTrust Appliance periodically monitors the virtualization platform configuration to ensure ongoing compliance with the above sub-requirements.

In the reference implementation, the configuration of VMware ESX 4.0 servers was performed in accordance with the HyTrust default PCI configuration template. Specifically, the following controls were configured and monitored:

All the boot services were disabled on the VMware ESX server except as follows:

```
S00microcode_ctl S00vmkstart S01vmware S02mptctlnode
S08iptables S09firewall S10network S12syslog S13irqbalance
S20random S55sshd S56rawdevices S56xinetd S58ntpd
S85gpm S85vmware-webAccess S90crond S91httpd.vmware
S99local S99pegasus S99vmware-autostart
```

Add following to each VM dot-vmx file:

```
isolation.tools.copy.enable=false
isolation.tools.paste.enable=false
isolation.tools.setGUIOptions.enable=false
```

Required set-uid programs:

```
pam_timestamp_check, passwd, pwdb_chkpwd, su, unix_chkpwd, vmkload_app, vmware-authd,
vmware-vmx
```

Optional:

```
crontab, ping, sudo, vmkping
```

Special case:

```
ssh-keysign
```

Make sure there is at least one user in the wheel group, then uncomment:

```
"auth required /lib/security/$ISA/pam_wheel.so
use_uid" in /etc/pam.d/su
```

Additionally, HyTrust establishes a system for rotating root passwords for the VMware ESX servers under HyTrust protection and allowing authorized users to check out one-time use time-limited auto-generated root passwords.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  HyTrust Appliance is a closed system based on the CentOS operating system, which implements a limited number of necessary services. Additional security features include the following:

  - Production services run unprivileged
  - No root login is allowed
  - The HTA administrator account is unprivileged
  - Sudoers-based privilege escalation
  - All unencrypted services disabled by default

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for*

example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.

HyTrust Appliance has the capability to download security updates and fixes directly from the HyTrust web site. When this is enabled, updates are downloaded and installed automatically. Updates can also be distributed as ISO packages and installed manually. To prevent Trojan attacks, HyTrust updates and HTA licenses are signed and validated using public keys.

Updates provided via this facility include security updates to the CentOS, application stack, and software developed by HyTrust.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

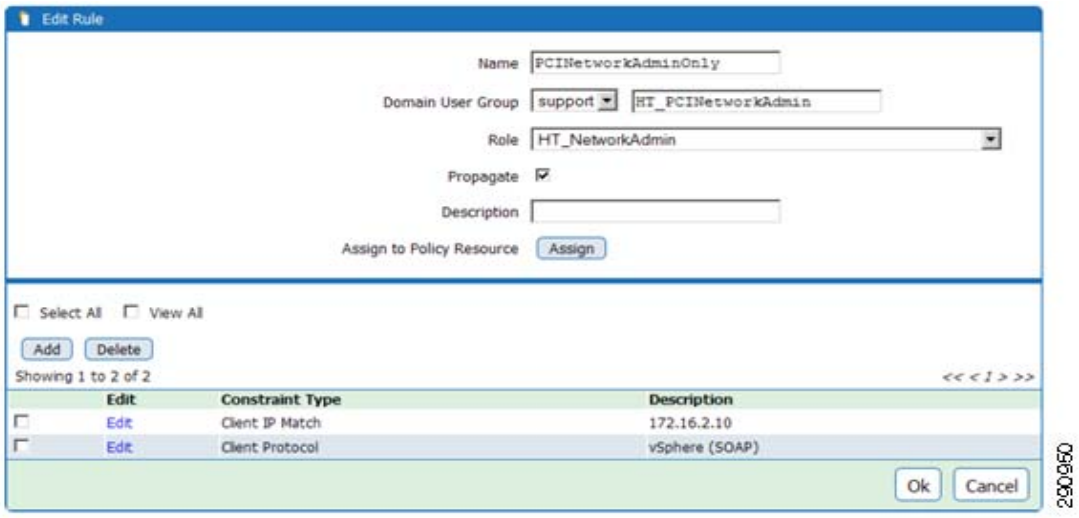
The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory, which is linked via LDAP, RADIUS, and TACACS+ services). Individual user IDs are assigned. Roles are defined and based on group membership. HyTrust Appliance connects to this resource via LDAP to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

  HyTrust Appliance implements a sophisticated policy-driven access control system that makes an authorization decision for every attempted operation in the Vblock environment. The authorization decision is based on the user ID as obtained from the vSphere session, the user function as derived from the user's assigned role in Active Directory, logical infrastructure segmentation, least privilege role defined for this activity, and object-level policy active for that user.

  In the reference implementation, a policy was created that restricted CDE virtual systems to operating only on the PCI portion of the infrastructure and enforced separation of duties between the network administrators and CDE application owners.

Figure 5-105 Edit Rule Screen



Policy and privilege definition was performed by a separate group of authorized users, typically security professionals.

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  HyTrust Appliance implements default "deny all" access policy. Many of the users that gain access to Vblock infrastructure by the means of HyTrust Appliance proxying their operations do not have privileges to log into the HyTrust Appliance management console.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing LDAP to the domain controller for AAA services and Microsoft Active Directory policy for user account services. Configure AAA services as shown in Requirement 7.

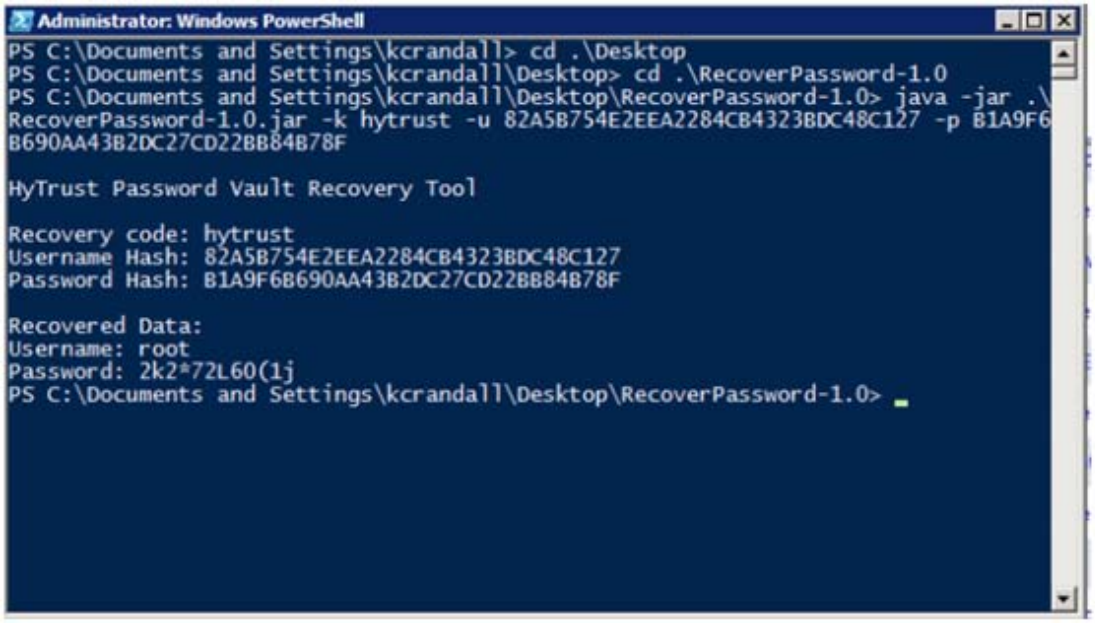
- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Sub-requirement 8.2 is met by supporting RSA two-factor authentication where the user enters the AD password (something they know) in conjunction with an RSA physical token (something they have).

  HyTrust Appliance acts as a compensating control for the Vblock infrastructure and enables RSA two-factor authentication to work with any methods of access to VMware vSphere or Cisco Nexus 1000V.
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  HyTrust Appliance enforces the use of one-time root passwords for all VMware ESX hosts in the environment. Unique random machine-generated passwords of 12 characters in length are set up for each host and rotated every five days (see Figure 5-106). If requested by a privileged user, a different one-time use password was generated and remained valid for a fixed time duration not to exceed 24 hours. Sub-requirement 8.5.8 was met by allowing only one temporary use password to be issued at the time, thus associating the password with a specific user who was issued the password.

Figure 5-106 Using Root Passwords



- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Sub-requirements 8.1, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, and 8.5.15 were met by integrating HyTrust Appliance authentication with Microsoft Active Directory. User accounts and passwords are not managed on HyTrust Appliance; instead, when authentication is requested by the user, HyTrust Appliance performs the actual authentication request against Active Directory. Complex AD environments with multiple domains are supported for authentication.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

HyTrust Appliance is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*

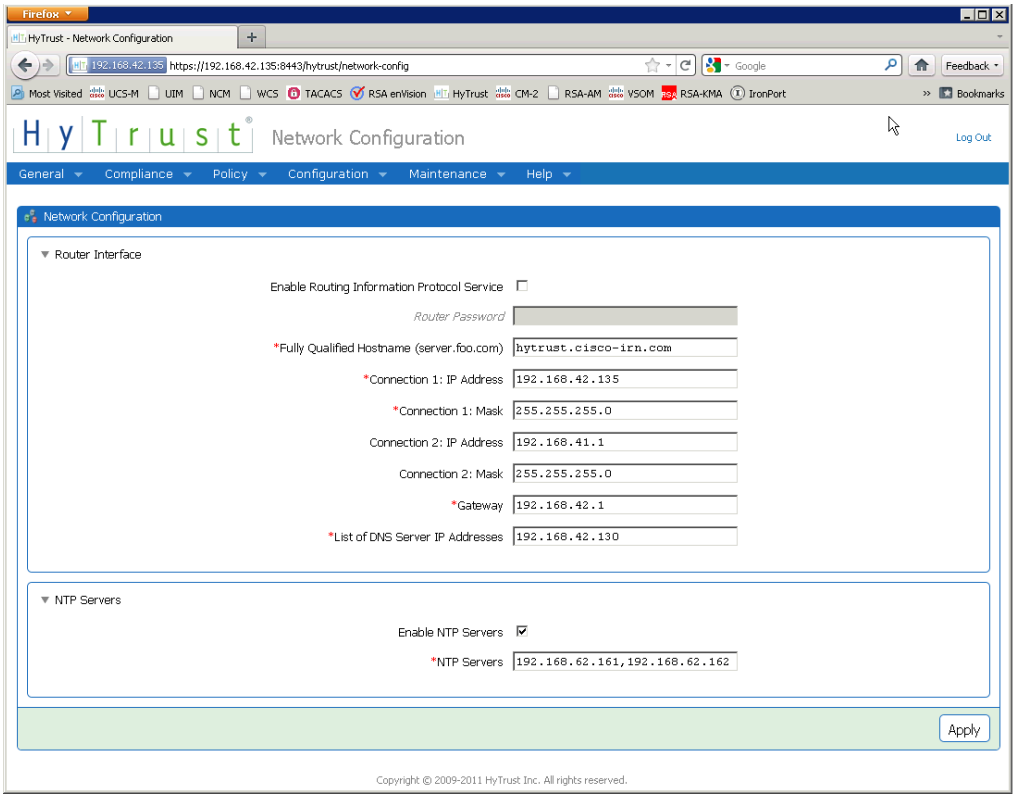
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

HyTrust Appliance uses NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. The HyTrust Appliance uses NTP to meet these requirements by specifying the NTP server in the IP settings. (See Figure 5-107.)

Figure 5-107 Specifying the NTP Server



- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Additional In Scope Devices

Any system that stores, processes, or transmits cardholder data is considered in scope for PCI compliance. Infrastructure components that provide network services such as load balancing or WAN optimization are often not considered when contemplating compliance. However, if these technologies pass sensitive data, they are subject to the same controls of traditional security products.

The capabilities that these components need to meet are highlighted in Table 5-1.

Infrastructure

Routing

Router—Branch

The Cisco Integrated Services Router (ISR) is the component that is used as the primary routing and security platform of the branches. It can securely scale to the requirements of the business because it has integrated firewall, VPN, and IPS/IDS capabilities. WAN options include traditional terrestrial paths using T1, T3, Ethernet, and so on; wireless options include 3G/4G/Wi-Fi modules connecting branches over public paths for higher availability.

The Cisco ISR consolidates voice, data, and security into a single platform with local and centralized management services. It delivers scalable rich media, service virtualization, and energy efficiency ideal for deployments requiring business continuity, WAN flexibility, and superior collaboration capabilities. The Cisco ISR uses field-upgradeable motherboards, with services such as security, mobility, WAN optimization, unified communications, video, and customized applications.

Table 5-36 lists the performance of the Cisco ISR in satisfying PCI sub-requirements.

Table 5-36 PCI Assessment Summary—Cisco ISR

Models Assessed	
CISCO891W version c890-universalk9-mz.151-3.T.bin	
CISCO1941W-A/K9 version c1900-universalk9-mz.SPA.151-3.T.bin	
CISCO2921/K9 version c2900-universalk9-mz.SPA.151-3.T.bin	
CISCO2951/K9 version c2951-universalk9-mz.SPA.151-3.T.bin	
CISCO3945-SPE150/K9 version c3900-universalk9-mz.SPA.151-3.T.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.1, 1.2.2, 1.2.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 4	4.1
PCI 6	6.1
PCI 7	7.7.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10. 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1,10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.4
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of the Cisco ISR is the segmentation of PCI scope and enforcement of that new scope boundary.

It has five primary functions/capabilities in relation to PCI.

1. As a router, directing traffic between networks

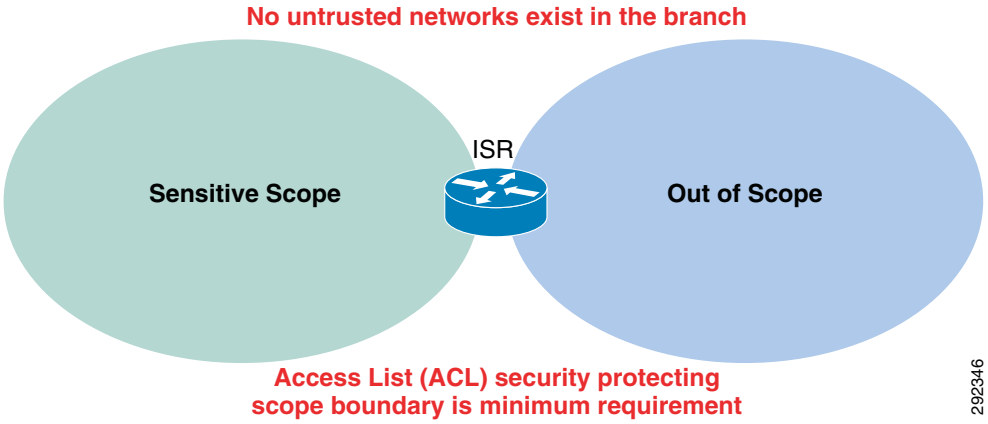
   A router in its simplest form routes between networks. By segmenting a network into sub-networks, an organization can isolate sensitive information from non-sensitive information. The Cisco ISR can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's cardholder data environment. Depending on risk vectors within the branch, different levels of enforcement might be required at the segmented scope boundary level. (See items 2, 3 and 4 following.)

2. As a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network

   A router with ACLs can be used to enforce segmented traffic only if the ACLs are used to filter and segment private networks of the organization. They may not be used to filter untrusted networks. For example, many organizations have a central chokepoint in their data center that is the connection to the Internet (an untrusted network). As long as the organization has only untrusted network

connections outside of the branch, (the data center, in this case), then an organization may use router access lists to protect its scope from its own private internal networks. As soon as the branch connects to untrusted networks directly, items 3 and 4 below become relevant. (See Figure 5-108.)

Figure 5-108 ACLs Segment Traffic



3. As a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network

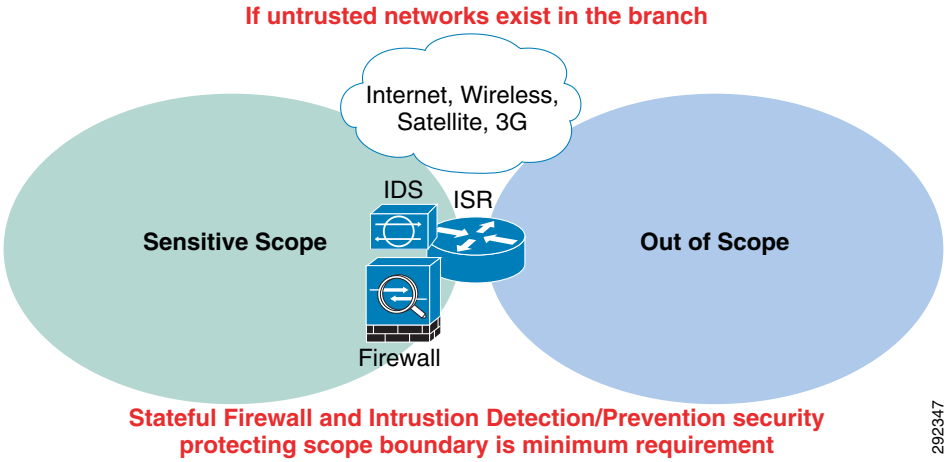
   As soon as any untrusted network is introduced at the branch level, firewalling and IDS/IPS must be deployed. The following are examples of untrusted networks:

   - The Internet
   - Wireless
   - Satellite
   - 3G/4G cellular backup

4. As an intrusion prevention system, inspecting all traffic going to and from the cardholder data environment

   As soon as any untrusted network is introduced at the branch level, firewalling and IDS/IPS must be deployed. (See Figure 5-109.)

Figure 5-109 Using Firewall and IDS/IPS



The Cisco ISR can be used to address segmentation challenges and enforce scope boundaries depending on the levels required by the organization. Each of these features can be enabled by using a license key. This feature is particularly useful for organizations because it does not require a visit to every branch to enable the firewall/IPS/IDS capability. If these capabilities are not used within the Cisco ISR, an external component(s) can be used to address this level of scope enforcement.

5. As a VPN system, encrypting all traffic going to and from the branch across open and public networks.

   The Cisco ISR can be used to address the need to encrypt the transmission of cardholder data across open, public networks such as 3G/4G/Wi-fi, and satellite technologies using SSL and IPSec technologies.

Table 5-37 lists the component assessment details for the Cisco ISR.

Table 5-37 Component Capability Assessment—Cisco ISR



ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- The security features of the Cisco ISR routers in the branch designs are configured using Cisco Security Manager. When adopting this as the primary method of router configuration, Cisco does not recommend making changes directly to the command-line interface (CLI) of the router. Unpredictable results can occur when central and local management are used concurrently.
- The general configuration of the Cisco ISR routers in the branch architectures are maintained with Cisco Prime LMS.

- Firewall rule sets must adhere to a “least amount of access necessary” policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment (for example, point-of-sale) networks.
- Ensure that inspection rules and/or zones are enabled on the Cisco ISR router so that the firewall maintains state (none are enabled by default).
- Redundant Cisco IOS firewalls do not have the capability to maintain state between the routers. During a failure, client communication sessions need to be re-established through the alternate router. If high availability with statefulness is a requirement, Cisco ASA firewalls should be used.
- Access into a branch router from the WAN needs to be protected by a branch-located firewall filter if the WAN technology is considered untrusted/public (for example, Internet DSL or cable network, public 3G or 4G, satellite). In the Cisco PCI Solution lab, a private MPLS WAN is simulated, and filtering of the branch traffic occurs on the WAN link of all in-scope locations.
- Disable the HTTP server service on the router and enable the HTTP secure server.
- Disable use of Telnet and enable use of only SSH version 2.
- Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, VTY, and line interfaces on the router. Disable the AUX interface.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the router.
- Change default passwords and community strings to appropriate complexity.
- Configure logs to be sent to a centralized syslog server, such as RSA enVision.
- Configure NTP to ensure all logging is coordinated.
- Disable un-necessary services (for example, Bootp, Pad, ipv6).
- Shutdown unused interfaces.

Each of the branch designs was implemented using guidance from the following:

- Cisco Enterprise Branch Security Design Guide—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/E_B_SDC1.html
- Branch/WAN Design Zone—
http://www.cisco.com/en/US/netsol/ns816/networking_solutions_design_guidances_list.html

Additional information for router hardening can be found at the following URLs:

- Cisco Guide to Harden Cisco IOS Devices—
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
- Cisco IOS Security Configuration Guide, Release 12.4—
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco zone-based firewalls are configurable to restrict traffic through the use of class map, policy map, and zone pair service policy statements and access lists.

- **PCI 1.2.2**—*Secure and synchronize router configuration files*

  Router configuration files are backed up centrally using Cisco Prime LMS. This tool also verifies that running and startup configurations of routers and switches are synchronized.

- **PCI 1.2.3**—*Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.*

  Cisco zone-based firewalls are configured with source and destination zones to control traffic passing from one zone to another. Each of these zone pairs receives a service policy, which is the mechanism that identifies permitted traffic, while all other traffic is dropped and logged.

```
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
```

- **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*

  Router WAN interfaces connected to public network connections such as the Internet should have filtering applied to prevent spoofing of both public and private IP address. Typical filters for private IP address blocks are as follows:

```
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark ------------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Your assigned IP's at edge---
 deny   ip <YOUR_CIDR_BLOCK> any log
 remark -
 remark ---Allow remaining public internet traffic---
 permit ip any any
```

- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*

Cisco zone-based firewalls are configured with source and destination zones to control traffic passing from one zone to another. Each of these zone pairs receives a service policy, which is the mechanism that identifies permitted traffic, while all other traffic is dropped and logged.

```
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
```

- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*

  Cisco zone-based firewalls are configurable to perform stateful inspection by use of the *inspect* statement in the associated class map, policy map, and zone pair service policy statements.

```
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp

policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log

zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
```

- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*

  In the branch design, VLANs are used to segment traffic based on function and security requirements. Each of these VLANs are assigned to an appropriate security zone using the zone-based firewall feature of the router.

```
interface GigabitEthernet0/0.11
 description POS
 zone-member security S_POS
interface GigabitEthernet0/0.13
 description VOICE
 zone-member security S_Voice
```

- **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco routers can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management, IPsec VPN for remote connectivity, and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists.

```
no ip http server
ip http secure-server
```

```
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 transport preferred none
 transport input ssh
 transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco routers have several services that are enabled by default that need to be disabled:

```
no service pad
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
no mop enable
no service finger
no ip forward-protocol nd
no ip http server
```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco routers support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

Note Strong cryptography—Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Before Crypto keys can be generated hostname and domain name must be entered

hostname R-A2-Small-1
ip domain name cisco-irn.com

! Generate keys with 1024 or larger bit key generation NOT the default 512

Crypto key generate rsa

ip ssh version 2

ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*

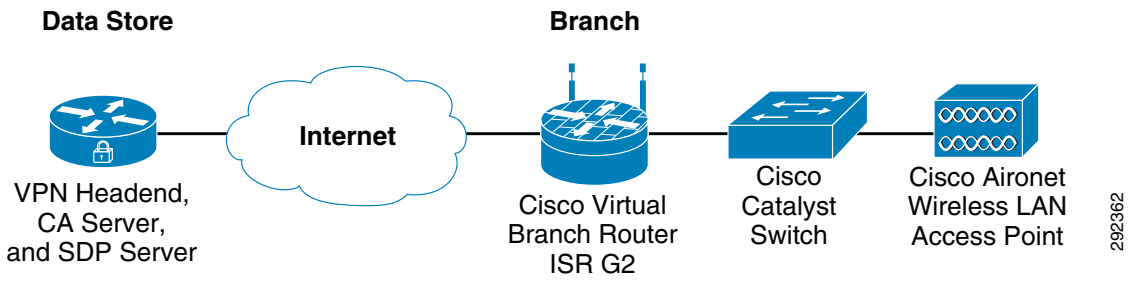
- *The Internet*
- *Wireless technologies,*
- *Global System for Mobile communications (GSM)*
- *General Packet Radio Service (GPRS)*

Public WAN link connections include technologies such as DSL, cable, satellite, Wi-Fi, and 3G/4G networks. These are considered untrusted public networks within PCI. A VPN is required to securely tunnel traffic between the branch and the enterprise network.

Cisco Virtual Office provides reference designs for building a VPN solution to connect branches to data centers using these technologies. For more information about Cisco VPN solutions, see: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6808/prod_white_paper0900aecd8051bf3b_ns855_Networking_Solutions_White_Paper.html

The following example describes equipment located at the branch and the data center headend router. The branch router is referred to as the spoke router, and the data center router as the hub. Figure 5-110 shows a simplified Cisco VPN topology.

Figure 5-110 Cisco VPN Topology



Cisco VPN technology connects the branches to the data center over the Internet. As a result, a secure, encrypted tunnel is used to secure sensitive information such as cardholder data. Cisco VPN technologies offer a choice to protect the data in transit and provide a secure access to the branches' networks, including Easy VPN and Dynamic Multipoint VPN (DMVPN).

This example shows DMVPN as the VPN technology. DMVPN uses IPSec-encrypted GRE tunnels, with dynamic routing. Two simultaneously active DMVPN tunnels are built from each branch to different hub routers, providing instant failover. If the primary tunnel fails, routing converges to use the secondary tunnel, and all sessions are kept alive. In addition, with DMVPN, branch routers can dynamically build spoke-to-spoke tunnels between each other to exchange data, without having to tunnel the traffic back to the hub, thus alleviating the load on the headend.

Following are sample DMVPN spoke and hub configurations. Enhanced Interior Gateway Routing Protocol (EIGRP) is used as the routing protocol inside the DMVPN network. Split-tunneling is used and only traffic on the POS and employee VLANs going to the servers on the 10.0.0.0 network at the headquarters is sent through the DMVPN tunnel, while any other traffic is sent straight to the Internet. Note that, if split-tunneling is not required, a default route (to 0.0.0.0) can be advertised from the hubs to the spokes, instead of specific subnets.

891 Branch Router

```
!! Configure the IP addresses on the VLAN interfaces
interface vlan 10
  description POS VLAN
  ip address 172.16.10.1 255.255.255.0
  no autostate
interface vlan 20
```

```
  description employee VLAN
  ip address 172.16.20.1 255.255.255.0
  no autostate
interface vlan 30
  description guest VLAN
  ip address 172.16.30.1 255.255.255.0
  no autostate
!! Configure the ISAKMP and IPSec policies
crypto isakmp policy 1
  encryption aes 256

crypto isakmp keepalive 35 5
crypto isakmp nat keepalive 10
crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
 mode transport

crypto ipsec profile cvs
 set transform-set t1
ip multicast-routing
!! Configure the DMVPN tunnel
interface Tunnel0
  bandwidth 1000
  ip address 192.168.1.3 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip hello-interval eigrp 99 30
  ip hold-time eigrp 99 90
  ip pim sparse-dense-mode
  ip nhrp map multicast <Primary-hub-public-IP>
  ip nhrp map 192.168.1.1 <Primary-hub-public-IP>
  ip nhrp nhs 192.168.1.1
  ip nhrp map multicast <Secondary-hub-public-IP>
  ip nhrp map 192.168.1.2 <Secondary-hub-public-IP>
  ip nhrp nhs 192.168.1.2
  ip nhrp authentication <password>
  ip nhrp network-id 12345
  ip nhrp holdtime 300
  ip nhrp registration no-unique
  ip nhrp shortcut
  ip nhrp redirect
  ip tcp adjust-mss 1360
  load-interval 30
  delay 1000
  qos pre-classify
  tunnel source GigabitEthernet0
  tunnel mode gre multipoint
  tunnel key 12345
  tunnel protection ipsec profile cvs


!! Configure the DMVPN routing protocol. Only permit the POS and employee LAN !!
subnets to be advertised to the hubs
ip access-list standard dmvpn_acl
  permit 172.16.10.0 0.0.0.255
  permit 172.16.20.0 0.0.0.255

router eigrp 99
  no auto-summary
  network 192.168.1.3 0.0.0.0
  network 172.16.10.1 0.0.0.0
  network 172.16.20.1 0.0.0.0
  distribute-list dmvpn_acl out
```

3945E Hub Router:

```
!! Configure the ISAKMP and IPSec policies

crypto isakmp policy 1
  encryption aes 256

crypto isakmp keepalive 35 5
crypto isakmp nat keepalive 10

crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
  mode transport require

crypto ipsec profile cvs
  set transform-set t1

!! Enable multicast routing

ip multicast-routing

!! Configure the DMVPN tunnel. Use the same bandwidth metric for both primary !! and
secondary hubs, but a lower delay metric on the primary hub

interface Tunnel0

  bandwidth 2000
  ip address 192.168.1.1 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip pim sparse-dense-mode
  ip nhrp authentication <password>
  ip nhrp map multicast dynamic
  ip nhrp network-id 12345
  ip nhrp redirect
  ip tcp adjust-mss 1360
  no ip split-horizon eigrp 99
  delay 1000
  qos pre-classify
  tunnel source <Outside_Interface >
  tunnel mode gre multipoint
  tunnel key 12345
  tunnel protection ipsec profile cvs

!! Configure the DMVPN routing protocol. Only the 10.0.0.0 network is        !!
advertised to the spokes in this example (split-tunneling)

router eigrp 99
  no auto-summary
  network 192.168.1.1 0.0.0.0
  redistribute static route-map split_in
ip access-list standard split_in
  permit 10.0.0.0

route-map split_in permit 10
  match ip address split_in
```

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for*

example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Integrated Services Routers. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco routers are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco routers, no users are allowed access unless specifically configured and assigned appropriate passwords.

```
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration, as specified in PCI requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

These AAA authentication groups are assigned to the administrative interfaces where users connect:

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

Services provide on-going access to software updates and security patches for a variety of Cisco products.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

The router is able to meet some of the requirements locally, as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco routers support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco routers require setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the routers also support the use of AES encryption of pre-shared keys.

  ```
  service password-encryption
  password encryption aes
  ```

  Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fall back user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  ```

```
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time, user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco routers support the ability to specify a minimum password length for local accounts.

  ```
  security passwords min-length 7
  ```

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco routers do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco routers do not support an automated capability to perform this function at this time: user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco routers support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco routers support the local ability to block logins after a specified time after failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco router management interfaces are configured as follows to meet this requirement:

  ```
  ip http timeout-policy idle 900

  line con 0
   session-timeout 15 output
   exec-timeout 15 0
  line vty 0 4
   session-timeout 15  output
   exec-timeout 15 0
  line vty 5 15
   session-timeout 15  output
   exec-timeout 15 0
  ```

Note If only the **session timeout** command is specified, the session timeout interval is based solely on detected input from the user. If the **session timeout** command is specified with the **output** keyword, the interval is based on both input and output traffic. You can specify a session timeout on each port. The **session-timeout** command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state. You can use a combination of the **exec-timeout** and **session-timeout** line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the **session-timeout** command causes on physical lines.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco ISRs are able to track and monitor all administrative user access and events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco routers track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
```

```
logging enable
notify syslog contenttype plaintext
hidekeys
```

The Cisco ISR uses Network Time Protocol (NTP) to update and synchronize their local clock facilities and meet sub-requirements 10.4.1 through 10.4.3:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco routers use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

  To learn more about NTP, visit the following URL: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using RSA enVision, a central logging repository that collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4**—*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.*

  Cisco routers are capable of performing intrusion detection. Each of the branch reference designs includes untrusted networks (either a public Internet connection or wireless networks); therefore, intrusion detection capabilities are required. IPS signature updates and configurations are managed centrally through Cisco Security Manager, which implements the following configuration statements to enable the IPS inspection capability in the routers:

```
ip ips config location flash0: retries 1 timeout 1
ip ips notify SDEE
ip ips name Store-IPS
!
ip ips signature-category
  category all
```

```
   retired true
  category ios_ips default
   retired false
!
interface GigabitEthernet0/0
 description WAN
 ip ips Store-IPS in
 ip ips Store-IPS out
interface GigabitEthernet0/1.11
 description POS
 ip ips Store-IPS in
 ip ips Store-IPS out
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 ip ips Store-IPS in
 ip ips Store-IPS out
```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Routers—Data Center

The primary function of data center routers from a PCI perspective is routing between sensitive networks and out-of scope networks. Data center routers function as WAN aggregation routers or connecting to larger networks such as the Internet. Therefore, performance and scalability are equally important as securely passing data. For this reason, and unlike the routers in the branch, security functions are typically separated physically into distinct appliances. The Cisco ASR1002 routers were used for the Internet edge and branch WAN edge portions of the network within the solution testing.

Primary PCI Function

The main function of the data center routers is the segmentation of PCI scope and enforcement of that new scope boundary. The data center router has four primary functions/capabilities in relation to PCI:

1. As a router, directing traffic between networks

   A router in its simplest form routes between networks. By segmenting a network into sub-networks, an organization can isolate sensitive information from non-sensitive information. Data center routers can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's cardholder data environment. Depending on risk vectors, different levels of enforcement might be required at the segmented scope boundary level. (See items 2, 3, and 4 following.)

2. As a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network

   A router with ACLs can be used to enforce segmented traffic only if the ACLs are used to filter and segment private networks of the organization. They may not be used to filter untrusted networks. For example, if a data center router is used to segment sensitive PCI networks from internal inventory networks, an organization may use router access lists to protect its scope. As soon as the branch connects to untrusted networks directly, items 3 and 4 below become relevant.

3. As a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network

   As soon as any untrusted network is introduced to the connections of the data center router, firewalling and IDS/IPS must be deployed. The following are examples of untrusted networks:

   - Internet
   - Wireless
   - Satellite
   - Cellular backup

4. As an intrusion prevention system, inspecting all traffic going to and from the cardholder data environment

   As soon as any untrusted network is introduced to the connections of the data center router, firewalling and IDS/IPS must be deployed at that location.

Table 5-38 PCI Assessment Summary—Data Center Routers

Models Assessed	
ASR-1002 (RP1) version asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.2, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8
PCI 2	2.2, 2.2.2, 2.2.3, 2.2.4, 2.3
PCI 4	4.1
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The data center routers protect trusted networks from untrusted networks with ACLs or firewall/IDS/IOS. (1.2, 1.3, 11.4)

Table 5-39 lists the component assessment details for the Cisco data center routers.

Table 5-39 Component Capability Assessment—Data Center Routers

Data Center Routers

PRIMARY FUNCTION
Protect trusted networks from untrusted networks with ACLs or firewall/IDS IOS

REQUIREMENT: 1, 11 (1.2, 1.3, 11.4)

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Configuration was done manually on the router CLI, and backup of configuration and monitoring of configuration for changes and non-compliance were done through Cisco Prime LMS (alternatively, CiscoWorks Resource Manager Essentials, a component of Cisco LMS, can be used as well).
- The perimeter firewalling of the data center was provided by the Cisco ASA. As a result, the Cisco Cisco ASR1002 was not evaluated according to the set of 1.x requirements for firewalls.
- Disable the HTTP server service on the router and enable the HTTP secure server.
- Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, VTY, and line interfaces on the router. Disable the AUX interface.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the router.
- Enable anti-spoofing on all interfaces.

- Routers in the data center were implemented using guidance from the following:
  - Enterprise Data Center Design guide based on a Data Center 3.0 Architecture—http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html
  - Enterprise Internet Edge Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html
- For the Internet edge routers, use the access list below on the interface that is facing the Internet. This access list explicitly filters traffic destined for the infrastructure address space. Deployment of edge infrastructure access lists requires that you clearly define your infrastructure space and the required/authorized protocols that access this space. The access list is applied at the ingress to your network on all externally facing connections, such as peering connections, customer connections, and so forth.

```
!
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark ------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Your assigned IP's at edge---
 deny   ip <YOUR_CIDR_BLOCK> any log
 remark -
 remark ---Allow remaining public internet traffic---
 permit ip any any
!
```

Note The **log** keyword can be used to provide additional details about source and destinations for a given protocol. Although this keyword provides valuable insight into the details of access list hits, excessive hits to an access list entry that uses the **log** keyword increase CPU utilization. The performance impact associated with logging varies by platform.

The service provider network in the solution represented an Multiprotocol Label Switching (MPLS) network. At the writing of this document, MPLS is considered a private network, and secure tunneling across the WAN is not required. MPLS implementations may be public or private with regards to PCI, depending on how the service provider implements the MPLS network and whether the provider has satisfactorily completed their annual PCI audit. For best practices when in doubt, Cisco recommends VPN tunneling be implemented. For further information on implementing an IPSec VPN, see the *IPSec VPN Direct Encapsulation Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Dir_Encap.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

Router configuration files are backed up centrally using Cisco Prime LMS. This tool also verifies that running and startup configurations of routers and switches are synchronized.

- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*

  PCI 1.3.8—*Do not disclose private IP addresses and routing information to unauthorized parties.*

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco routers can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management, IPsec VPN for remote connectivity, and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists:

```
no ip http server
ip http secure-server
ip scp server enable
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 transport preferred none
 transport input ssh
 transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco routers have several services that are enabled by default that can be disabled:

```
no service pad
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
no mop enable
no service finger
no ip forward-protocol nd
no ip http server
```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco routers support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

Note Strong cryptography is based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Before Crypto keys can be generated hostname and domain name must be entered

hostname RWAN-1
ip domain name cisco-irn.com

! Generate keys with 1024 or larger bit key generation NOT the default 512

Crypto key generate rsa

ip ssh version 2

ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco routers. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco routers are configured to use a AAA model for user-based access. Users can be assigned to groups, and based on privilege levels, have access to only the information they require for their job function. By default in Cisco routers, no users are allowed access unless specifically configured and assigned appropriate passwords.

```
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

The following AAA authentication groups are assigned to the administrative interfaces where users connect:

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco routers to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure ACS must be implemented. Configure AAA services as shown above in Requirement 7.

The router is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco routers support the creation of local user accounts with unique ID's through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco routers require the setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the routers also support the use of AES encryption of pre-shared keys.

  ```
  service password-encryption
  password encryption aes
  ```

  Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

Cisco routers do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time, user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco routers support the ability to specify a minimum password length for local accounts.

  ```
  security passwords min-length 7
  ```

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco routers do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco routers do not support an automated capability to perform this function at this time: user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco routers support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco routers support the local ability to block logins after a specified time after failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco router management interfaces are configured as follows to meet this requirement:

  ```
  ip http timeout-policy idle 900

  line con 0
   session-timeout 15 output
   exec-timeout 15 0
  line vty 0 4
   session-timeout 15  output
   exec-timeout 15 0
  line vty 5 15
   session-timeout 15  output
   exec-timeout 15 0
  ```

Note If only the **session timeout** command is specified, the session timeout interval is based solely on detected input from the user.

If the **session timeout** command is specified with the **output** keyword, the interval is based on both input and output traffic.You can specify a session timeout on each port.

The **session-timeout** command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state.

You can use a combination of the **exec-timeout** and **session-timeout** line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the **session-timeout** command causes on physical lines.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco routers are able to track and monitor all administrative user access and events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco routers track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log
```

```
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

Cisco routers use NTP to update and synchronize their local clock facilities and meet sub-requirements 10.4 through 10.4.3.

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco routers use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

  To learn more about NTP, visit: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Note The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Switching

Switches—Branch

Cisco branch switches provide connectivity for wired endpoints and the ability to segment them onto their own sensitive scope networks. Virtual local area networks (VLANs) are used to put sensitive PCI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks.

Branch switches are broken into three categories to provide scale and feature relevance;

- Compact switches—Quiet, small form factor switches that can be used on branch floors to extend the capability of the network to the register. These switches use power over Ethernet (PoE) pass-through, reducing expensive power and network cabling costs to new devices at the area of sale.
- Access switches—Stackable, expandable switches that can be used for wired device port density in the branch wiring closets. Access switches offer a variety of modular and fixed configuration options, and feature operational efficiency with StackPower, FlexStack, and NetFlow to increase visibility and control.
- Core/distribution—Highly redundant, powerful core switches allow for the most demanding business requirements of the branch. Modular functionality provides the ability to insert security technology as the needs of the business expand into new areas.

Table 5-40 PCI Assessment Summary—Branch Switches

Models Assessed	
WS-C2960PD-8TT-Lc2960-lanbasek9-mz.122-55.SE1.bin WS-C2960G-8TC-Lc2960-lanbasek9-mz.122-50.SE4.bin WS-C2960-8TC-Lc2960-lanbasek9-mz.122-50.SE4.bin WS-C2960S-48FPS-Lc2960s-universalk9-mz.122-53.SE1.bin WS-C3750X-48PF-Sc3750e-universalk9-mz.122-53.SE2.bin WS-C2960CPD-8PT-Lc2960c405-universalk9-mz.122-55.0.43.SK.bin WS-4507+R SUP-7cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin WS-C3560X-48PF-Sc3560e-universalk9-mz.122-53.SE2.bin WS-C3560CPD-8PT-Lc3560c405ex-universalk9-mz.122-55.0.44.SK.bin	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 9	9.1.2
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.1.b, 11.1.d
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

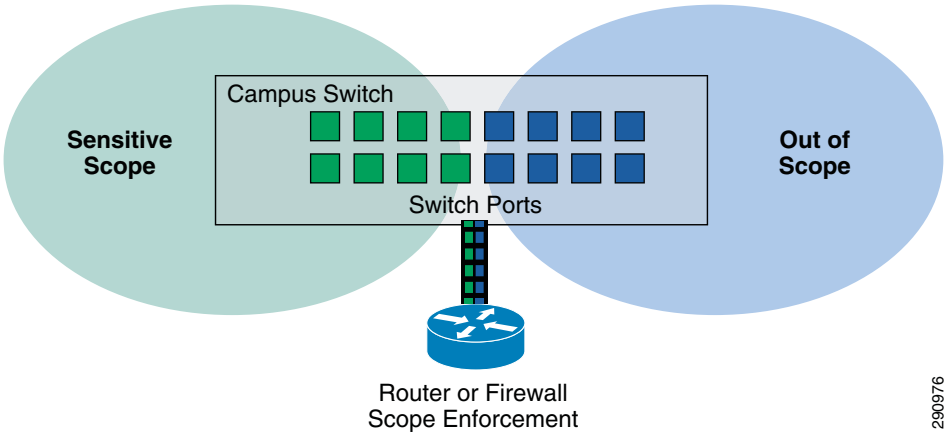
Primary PCI Function

The primary PCI compliance feature of branch switches is to provide secure wired port access. (9.1.2, 11.1)

Branch switches also provide PCI compliance via segmentation of sensitive networks from out-of-scope networks. Although technically a firewall or ACL is used to enforce PCI Requirement 1, switches extend that Layer 3 boundary to Layer 2. Using VLANs, Cisco branch switches allow organizations to put their payment networks into separate VLANs (scopes) from other non-sensitive data (out-of-scope).

Figure 5-111 shows an example of switch segmentation.

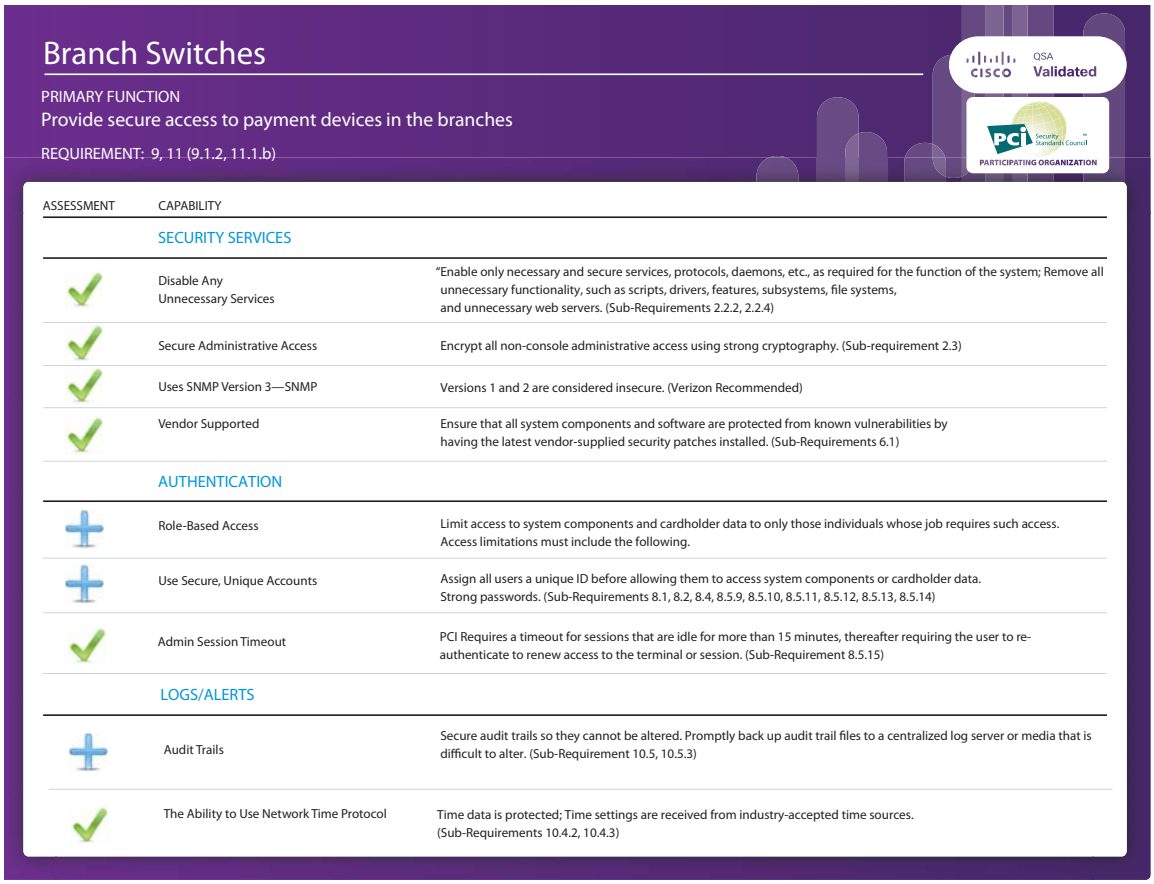
Figure 5-111 Cisco Branch Switch Segmentation



Although the enforcement of these boundaries would be handled by either a router or firewall, the switch provides the port density and access required to connect the payment devices from the branch floor.

Table 5-41 lists the component assessment details for the Cisco branch switches.

Table 5-41 Component Capability Assessment—Branch Switches



Branch Switches

PRIMARY FUNCTION
Provide secure access to payment devices in the branches

REQUIREMENT: 9, 11 (9.1.2, 11.1.b)

cisco QSA Validated

PCI Security Standards Council PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- The configurations of the Cisco Catalyst switches in the branch architectures are maintained within Cisco Prime LMS (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- The use of VLANs on the Cisco Catalyst switch enables the organization to provide same-box wired access to its devices while maintaining segregated addressing schemes.
- Disable the HTTP server on the switch and enable the HTTP secure server.
- Using the stacking capability of Cisco Catalyst switches improves high availability designs while simplifying configuration and support.
- Cisco SmartPorts simplifies connecting the right device to the right VLAN.
- Network Admission Control (NAC) protects the network from rogue devices being connected.
- Cisco compact switches can easily add more securely managed ports where needed (for example, Cash Wrap and customer service desk), and some models can use PoE.
- Set the **session** and **exec timeout** commands to 15 minutes or less.
- Configure appropriate banner messages on login, incoming, and exec modes of the switch. The login banner warning should not reveal the identity of the company that owns or manages the switch. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.

- Configure the primary login authentication of the switch to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the switch itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the switch.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco switches can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists.

```
no ip http server
ip http secure-server
ip scp server enable
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 transport preferred none
 transport input ssh
 transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco switches may have several services that are enabled by default that can be disabled.

```
no service pad
no service udp-small-servers
no service tcp-small-servers
no service finger
no ip http server
```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco switches support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

Note Strong cryptography—Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Before Crypto keys can be generated hostname and domain name must be entered

hostname S-A2-Small-1
ip domain name cisco-irn.com

! Generate keys with 1024 or larger bit key generation NOT the default 512

Crypto key generate rsa

ip ssh version 2

ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco switches. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

  For more information about PSIRT:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

To meet all of the requirements listed below, the PCI solution uses the centralized user database in Active Directory, which is linked to via LDAP, RADIUS, and TACACS+ services. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. This resource is used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*

- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco switches are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco switches, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

  Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

  These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco switches to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure ACS must be implemented. Configure AAA services as shown above in Requirement 7.

The switch is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco switches support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco switches require the setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the switches also support the use of AES encryption of pre-shared keys.

  ```
  service password-encryption
  password encryption aes
  ```

  Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco switches do not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco switches support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco switches support the local ability to block logins after a specified time after failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco switch management interfaces are configured as follows to meet this requirement:

  ```
  ip http timeout-policy idle 900

  line con 0
   session-timeout 15 output
   exec-timeout 15 0
  line vty 0 4
   session-timeout 15  output
   exec-timeout 15 0
  line vty 5 15
   session-timeout 15  output
   exec-timeout 15 0
  ```

Note If only the **session timeout** command is specified, the session timeout interval is based solely on detected input from the user. If the **session timeout** command is specified with the **output** keyword, the interval is based on both input and output traffic. You can specify a session timeout on each port. The **session-timeout** command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state. You can use a combination of the **exec-timeout** and **session-timeout** line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the **session-timeout** command causes on physical lines.

Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.2**—*Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.*

In addition to disabling switch port interfaces for ports that are not in use, or in public areas, ports can also be placed in the guest network VLAN. This VLAN is treated as a public network and requires the appropriate PCI requirements for public networks to be met as well (for example, IPS/IDS and stateful firewall). Cisco switches support a feature called SmartPorts, whereby devices connected to these ports can be dynamically moved to an appropriate network VLAN from a blackhole VLAN or guest VLAN based on automatic identification macros. This allows ports to be active for periodic use when devices are attached (for example, media players for in-aisle promotions, and IP phones for customer service) when these network ports are in publicly accessible areas. The following configurations show how to enable SmartPorts for a variety of default or custom devices based on MAC addresses as opposed to 802.1x authentication methods.

```
!
macro global description cisco-desktop
!
macro auto execute CISCO_LAST_RESORT_EVENT builtin CISCO_AP_AUTO_SMARTPORT
ACCESS_VLAN=17
macro auto execute Retail-POS builtin CISCO_PHONE_AUTO_SMARTPORT ACCESS_VLAN=11
VOICE_VLAN=13
macro auto execute POS-Systems remote scp://SMARTPORT@192.168.42.122/POS-Systems.txt
ACCESS_VLAN=11 VOICE_VLAN=13
!
macro auto mac-address-group Retail-POS
 oui list 001C26
 oui list 001C25
 mac-address list 0021.5C02.1DEF
 mac-address list 001C.25BE.99C2
macro auto device media-player ACCESS_VLAN=12
macro auto device ip-camera ACCESS_VLAN=20
macro auto device phone ACCESS_VLAN=17 VOICE_VLAN=13
macro auto device access-point ACCESS_VLAN=18
macro auto device lightweight-ap ACCESS_VLAN=18
!
macro auto global processing fallback cdp
!
interface GigabitEthernet0/9
 macro description CISCO_SWITCH_EVENT
```

More information about Cisco SmartPorts can be found at the following URL: http://www.cisco.com/en/US/docs/switches/lan/auto_smartports/12.2_55_se/configuration/guide/asp_cg.html

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events when using 802.1x.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*

  - **PCI 10.2.7**—*Creation and deletion of system-level objects*

- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco switches track individual administrator actions as identified in the requirement above (10.1, 10.2, and 10.3) through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

Cisco switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco switches use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

  To learn more about NTP, visit: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml



Note The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

Requirement 11: Regularly Test Security Systems and Processes

The following requirements can be addressed using Cisco Network Admission Control.

- **PCI 11.1.b**—*Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:*
  - *WLAN cards inserted into system components*
  - *Portable wireless devices connected to system components (for example, by USB, etc.)*
  - *Wireless devices attached to a network port or network device*
- **PCI 11.1.d**—*If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.*

  Cisco NAC capabilities can be configured on the branch switches to automate the verification of approved devices being attached to the network. In addition to configuring the NAC authentication services in the data center, add the following configurations to the switch and switch interface ports where NAC is to be used (for example, publicly accessible ports):

```
Pre-requirements for NAC (domain name, name server, time settings, crypto keys):
 ip domain-name cisco-irn.com
 ip name-server 192.168.42.130
 Crypto key generate rsa 1024
 ntp server 192.168.62.161 prefer
 ntp server 192.168.62.162
 clock timezone PST -8
 clock summer-time PDT recurring
!
! ----Configurations to add for NAC ----
!
aaa new-model
!
!
aaa authentication dot1x default group radius local
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 192.168.42.111
 server-key 7 <removed>
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
radius-server vsa send accounting
radius-server vsa send authentication
!
```

```
authentication mac-move permit
!
!
ip device tracking
ip admission name ise proxy http inactivity-time 60
!
cts sxp enable
cts sxp default source-ip 10.10.111.13 {use Switch Management IP}
!
dot1x system-auth-control
!
fallback profile ise
 ip access-group ACL-DEFAULT in
 ip admission ise
!
! ----Auto Smart Ports Macro method for port configurations-------
!
macro name dot1x
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout tx-period 5
```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Catalyst Switches—Data Center

The Cisco Catalyst family of data center switches securely switches data; from servers to high speed trunks, maintaining the integrity of segmented scopes of compliance. They provide scalable inter-switch connectivity, high port density for wired endpoints, and the ability to segment them into sensitive scope networks. VLANs are used to put sensitive PCI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks. Data center Cisco Catalyst switches are highly redundant, capable of delivering high performance switching, with feature options depending on the needs of the business.

Modular functionality provides the ability to insert security technology to enforce compliance needs.

- Security services include access control, firewall, and intrusion prevention.

- Wireless services can be aggregated into these switches for central policy control of unified wireless access points.
- Application services include quality of service (QoS), content filtering, and load balancing.

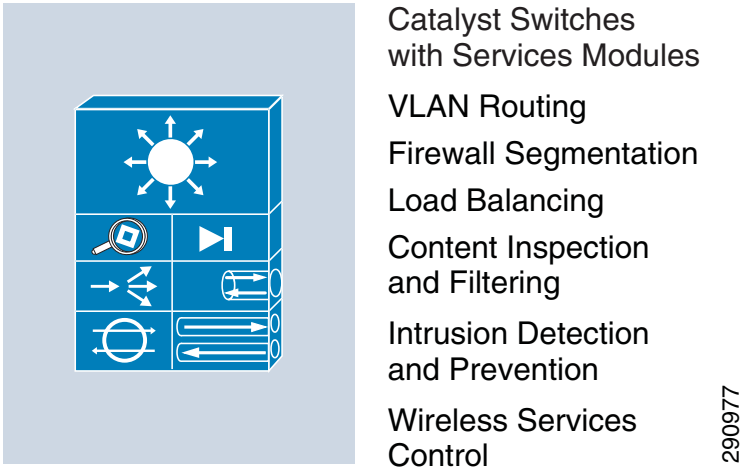
Table 5-42 PCI Assessment Summary—Cisco Catalyst Data Center Switches

Models Assessed	
Catalyst6509-Sup720-3BXL version s72033-adventerprisek9_wan-mz.122-33.SXJ.bin WS-C3750-48P version c3750-ipbasek9-mz.122-55.SE1.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.2
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 9	9.1.1
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary PCI compliance feature of Cisco Catalyst data center switches is securing the infrastructure. Cisco Catalyst switches have firewall/IDS modules for perimeter security. (See Figure 5-112.)

Figure 5-112 Cisco Catalyst Data Center Switches



The main function of the Cisco Catalyst data center switches is segmentation of PCI scope and enforcement of that new scope boundary. These switches have five primary functions/capabilities in relation to PCI:

- Using VLANs, Cisco Catalyst switches allow an organization to put its payment networks into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Catalyst switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, an organization can isolate sensitive information from non-sensitive information. The Cisco Catalyst switch can perform the ability to segment and route sensitive traffic from non-sensitive and reduce the overall scope of a company's cardholder data environment. Depending on risk vectors, different levels of enforcement are required at the segmented scope boundary level. See the following bullets for details.
- The Layer 3 Cisco Catalyst switch acts as a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network. A Cisco Catalyst switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the organization. ACLs may not be used to segment untrusted networks.
- The Cisco Catalyst switch with a firewall service module restricts traffic between the cardholder data environment and other areas of the network. As soon as any untrusted network is introduced, firewalling and IDS/IPS must be deployed.
- The Layer 3 Cisco Catalyst switch with an intrusion prevention module inspects all traffic going to and from the cardholder data environment. As soon as any untrusted network is introduced, firewalling and IDS/IPS must be deployed.

Table 5-43 lists the component assessment details for the Cisco Catalyst data center switches.

Table 5-43 Component Capability Assessment—Cisco Catalyst Data Center Switches

Cisco Catalyst Data Center Switches

QSA Validated

PRIMARY FUNCTION

Provide secure access to payment infrastructure and servers using VLANs, ACLs, and firewall/IPS

REQUIREMENT: 1, 11 (1.2, 1.3, 11.4)

PCI Security Standards Council PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- The configurations of the Cisco Catalyst switches in the data center and Internet edge architectures are maintained within Cisco Prime LMS (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- The use of VLANs on the Cisco Catalyst switch enables the organization to provide same-box wired access to its devices while maintaining segregated addressing schemes.
- Using the stacking capability of Cisco Catalyst switches improves high availability designs while simplifying configuration and support.
- Disable the HTTP server on the switch and enable the HTTP secure server.
- Set the **session** and **exec timeout** commands to 15 minutes or less.
- Configure appropriate banner messages on login, incoming, and exec modes of the switch. The login banner warning should not reveal the identity of the company that owns or manages the switch. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the switch to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the switch itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the switch.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Router and switch configuration files are backed up centrally using Cisco Prime LMS. This tool also verifies that running and startup configurations of routers and switches are synchronized.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco switches can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists.

```
no ip http server
ip http secure-server
ip scp server enable
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 transport preferred none
 transport input ssh
 transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco switches may have several services that are enabled by default that can be disabled.

```
no service pad
no service udp-small-servers
no service tcp-small-servers
no service finger
no ip http server
```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco switches support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for*

example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco switches. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco switches are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco switches, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa new-model
    aaa authentication login RETAIL group tacacs+ local
    aaa authentication enable default group tacacs+ enable
    aaa authorization exec default group tacacs+ if-authenticated
    aaa accounting update newinfo
    aaa accounting exec default start-stop group tacacs+
    aaa accounting commands 15 default start-stop group tacacs+
    aaa accounting system default start-stop group tacacs+
    aaa session-id common
    tacacs-server host 192.168.42.131
    tacacs-server directed-request
    tacacs-server domain-stripping
```

```
tacacs-server key 7 <removed>
```

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

The switch is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco switches support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco switches require setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the switches also support the use of AES encryption of pre-shared keys.

```
service password-encryption
password encryption aes
```

Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fall back user accounts.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco switches do not support the ability to specify a minimum password length for local accounts; this would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco switches support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco switches support the local ability to block logins after a specified time after failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco switch management interfaces are configured as follows to meet this requirement:

  ```
  ip http timeout-policy idle 900
  ```

```
line con 0
 session-timeout 15 output
 exec-timeout 15 0
line vty 0 4
 session-timeout 15  output
 exec-timeout 15 0
line vty 5 15
 session-timeout 15  output
 exec-timeout 15 0
```

Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.1**—*Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a branch.*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events when using 802.1x.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco switches track individual administrator actions as identified in the requirement above (10.1, 10.2, and 10.3) through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
```

```
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

Cisco switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco switches use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

  To learn more about NTP, visit: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml



Note The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Nexus 1000V Switch—Data Center

The Cisco Nexus 1000V Series Switch provides connectivity for virtual servers with the ability to segment them onto their own sensitive scope networks. VLANs are used to put sensitive PCI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks.

The Cisco Nexus 1000V Series Switch provides advanced networking functions and a common network management model in a virtualized server environment. The Cisco Nexus 1000V Series Switch replaces the virtual switching functionality of the VMware vCenter data center container of servers. Each server in the data center container is represented as a line card in the Cisco Nexus 1000V Series Virtual Supervisor Module (VSM) and is managed as if it were a line card in a physical Cisco switch.

Key benefits of the Nexus 1000V include the following:

- Policy-based virtual machine (VM) connectivity
- Mobile VM security and network policy
- Non-disruptive operational model for your server virtualization, and networking teams

Table 5-44 PCI Assessment Summary—Cisco Nexus 1000V Series Switch

Models Assessed	
Cisco Nexus 1000V version 4.2(1)SV1(4)	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10. 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary PCI compliance feature of Cisco Nexus switches is secure aggregation and access layer connectivity.

- Using VLANs, Cisco Nexus switches allow an organization to put its payment network into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Nexus switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, an organization can isolate sensitive information from non-sensitive information. The Cisco Nexus switch can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's cardholder data environment. Depending on risk vectors, various levels of enforcement are required at the segmented scope boundary level.

- The Layer 3 Cisco Nexus switch acts as a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network. A Cisco Nexus switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the organization. ACLs may not be used to segment untrusted networks.
- The Cisco Nexus switch uses *virtualization contexts*, which are essentially virtualized switches. Each virtualized context has its own configuration and management interfaces that can be used to segregate not only data but administration as well.

Table 5-45 lists the component assessment details for the Cisco Nexus 1000V Series Switch.

Table 5-45 Component Capability Assessment—Cisco Nexus 1000V Series Switch

Cisco Nexus 1000V Series Switch

QSA Validated

PRIMARY FUNCTION
Secure aggregation and access layer connectivity

REQUIREMENT: 1

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

The Cisco Nexus 1000V Series Switch includes the Cisco Integrated Security features that are found on Cisco physical switches to prevent a variety of attack scenarios. For example, a rogue virtual machine can spoof its MAC and IP addresses so that it appears to be an existing production virtual machine, send a rogue Address Resolution Protocol (ARP) transaction mimicking the way that VMware vMotion announces the location of a migrated virtual machine, and divert traffic from the production virtual machine to the rogue virtual machine. With Cisco Integrated Security features, this type of attack can easily be prevented with simple networking policy. Because server virtualization is being used for desktop and server workloads, it is critical that this type of security feature be deployed for the proper operation of a virtualized environment.

The Cisco Nexus 1000V Series implementation has two main components:

- Virtual Supervisor Module (VSM)
- Virtual Ethernet module (VEM)

The Cisco Nexus 1000V VSM is installed as an appliance server on either a standalone Cisco UCS server (Cisco Nexus 1010) or as a virtual appliance on VMware ESXi server running on a blade of the Cisco UCS system.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  On the Cisco Nexus 1000V, you can turn off the unwanted services such as Telnet and HTTP.

  ```
  no feature http-server
  no feature telnet
  ```

  The remote access is restricted to SSH when you turn off the Telnet service.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  Cisco SMARTnet services provide ongoing access to software updates and security patches. Cisco Nexus 1000V update software includes fixes for security vulnerabilities along with other bug fixes. The software is available directly from the Cisco website.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database. It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*

- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  TACACS+ provides for separate authentication, authorization, and accounting services. The TACACS+ daemon provides each service independently.

  First, you have to enable the TACACS+ feature on the Cisco Nexus 1000V:

```
config t
feature tacacs+
```

  The following commands show how to configure the TACACS+ server:

```
tacacs-server key 7 password
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
aaa authentication login default group CiscoACS
```

  Number *7* in the key command specifies an encrypted string (key) to follow.

  Local is the default and is used when no methods are configured or when all the configured methods fail to respond. Configure the local user with encrypted passwords for fallback authentication:

```
username admin password 5 <removed>  role network-admin
username retail password 5 <removed>  role network-operator
```

  Both roles used in the **username** commands are pre-defined roles in the Cisco Nexus 1000V. The network admin role has access to all commands on the switch, whereas the network operator role has access to all read commands on the switch.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters. PCI Sub-Requirements with Compensating Controls*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Nexus Switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco Nexus switches track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging server 192.178.42.124 6 facility syslog

aaa accounting default group CiscoACS
```

Cisco Nexus switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center

site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco Nexus switches use NTP to meet these requirements by implementing the following configuration statements.

```
enable NTP
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management

clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
```

To learn more about NTP, visit: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Nexus Switches—Data Center

The Cisco Nexus family of data center switches securely switches data; from payment application servers to high speed trunks of the core, maintaining the integrity of segmented scopes of compliance. They provide scalable inter-switch connectivity and high port density for wired endpoints. VLANs are used to put sensitive PCI applications and devices onto their own network and segregate them from devices on non-sensitive networks.

Cisco Nexus switches are ideal for enterprise-class server and aggregation layer deployments. These multipurpose, multilayer switches can be deployed across a diverse set of traditional, virtualized, unified, and high-performance computing environments. They enable diverse transports over Ethernet (including Layer 2, Layer 3, and storage traffic) on one common platform. Nexus switches help transform your data center, with a standards-based, multipurpose, multiprotocol, Ethernet-based fabric.

Table 5-46 PCI Assessment Summary—Cisco Nexus Data Center Switches

Models Assessed	
Cisco Nexus5020 Chassis (“40x10GE/Supervisor”) version n5000-uk9.5.0.3.N1.1b.bin Cisco 7010 Chassis (“Supervisor module-1X”) version n7000-s1-dk9.5.1.2.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.2

Table 5-46 PCI Assessment Summary—Cisco Nexus Data Center Switches (continued)

PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10. 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary PCI compliance feature of Cisco Nexus data center switches is secure aggregation and access layer connectivity.

- Using VLANs, Cisco Nexus switches allow an organization to put its payment network into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Nexus switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, an organization can isolate sensitive information from non-sensitive information. The Cisco Nexus switch can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's cardholder data environment. Depending on risk vectors, various levels of enforcement are required at the segmented scope boundary level.
- The Layer 3 Cisco Nexus switch acts as a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network. A Cisco Nexus switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the organization. ACLs may not be used to segment untrusted networks.
- The Cisco Nexus switch uses virtualization contexts, which are essentially virtualized switches. Each virtualized context has its own configuration and management interfaces that can be used to segregate not only data but administration as well.

Table 5-47 lists the component assessment details for the Cisco Nexus data center switches.

Table 5-47 Component Capability Assessment —Cisco Nexus Data Center Switches

Cisco Nexus Data Center Switches

PRIMARY FUNCTION
Secure access to payment infrastructure and servers using segmentation of trusted networks (VLANs, ACLs)
REQUIREMENT: 1 (1.3.5)

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Configuration was done manually on the router CLI, and backup of configuration and monitoring of configuration for changes and non-compliance were done through the Cisco Prime LMS (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- Configure appropriate banner messages on login, incoming, and EXEC modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Nexus switches in the data center were implemented using guidance from the Enterprise Data Center Design guide based on a Data Center 3.0 Architecture:
  http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html

  Enterprise Internet Edge Design Guide:
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html
- The Cisco Nexus 7010 and the Cisco Nexus 5000 were used for the aggregation block portions of the lab validation network.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Cisco Nexus configuration files are backed up centrally using Cisco Prime LMS. This tool also verifies that running and startup configurations are synchronized.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco Nexus switches can be configured to use secure protocols for all system functions. This includes SSH for remote management, SCP, and SFTP for file transfers. Insecure services can be disable or blocked using configuration statements and access lists.

```
no feature telnet
no telnet server enable
feature ssh
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Nexus switches have no extraneous services that are enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco Nexus switches support administrative protocols with strong cryptography such as SSH version 2.

Note Strong cryptography—Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Generate keys with 1024 or larger bit key generation NOT the default 512

ssh key rsa 1024 force

! Cisco Nexus switches utilize SSH version 2.
```

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

Cisco SMARTnet services provide ongoing access to software updates and security patches: http://www.cisco.com/cisco/software/type.html?mdfid=282099479&flowid=3088.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco Nexus switches are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels have access to only the information they require for their job function. By default in Cisco Nexus switches, no users are allowed access unless specifically configured and assigned.

```
feature tacacs+

aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username admin password 5 <removed>  role network-admin
username retail password 5 <removed>  role network-admin
username bart password 5 <removed>  role network-admin
username emc-ncm password 5 <removed>  role network-admin
```

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco Nexus switches to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure Access Control Server must be implemented. Configure AAA services as shown above in Requirement 7.

The switch is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco Nexus switches support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts. They should be individually unique as specified by policy.

```
username admin password 5 <removed>  role network-admin
username retail password 5 <removed>  role network-admin
username bart password 5 <removed>  role network-admin
username emc-ncm password 5 <removed>  role network-admin
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco Nexus switches support the ability to specify a password.

```
username admin password 5 <removed>  role network-admin
username retail password 5 <removed>  role network-admin
username bart password 5 <removed>  role network-admin
username emc-ncm password 5 <removed>  role network-admin
```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Local user fall back accounts are created with the **username** command and use MD5-encryption for the user password. Communication to the AAA server using RADIUS or TACACS+ is encrypted when using centralized authentication.

```
username admin password 5 <removed>  role network-admin
username retail password 5 <removed>  role network-admin
username bart password 5 <removed>  role network-admin
username emc-ncm password 5 <removed>  role network-admin
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco Nexus switches do not support an automated capability to perform this function at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco Nexus switches do not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS.

Requirements 8.5.10–8.5.11 can be satisfied with a single configuration statement as identified below.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.PCI Sub-Requirements with Compensating Controls*

  The NX-OS software accepts only strong passwords when you have password strength checking enabled (default) using the **password strength-check** command. The characteristics of a strong password include the following:

  - At least eight characters long
  - Does not contain many consecutive characters (such as “abcd”)
  - Does not contain many repeating characters (such as “aaabbb”)
  - Does not contain dictionary words
  - Does not contain proper names
  - Contains both uppercase and lowercase characters
  - Contains numbers

  ```
  password strength-check
  ```

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco Nexus switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco Nexus switches do not support the ability to lock out local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco Nexus switches do not support the ability to manage lockout of local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco Nexus switch management interfaces are configured as follows to meet this requirement:

  ```
  line console
    exec-timeout 15

  line vty
    exec-timeout 15
  ```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Nexus switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*

  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco Nexus switches track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging server 192.168.42.124 6
!
! --- for implementations using VRF's ----
!
logging server 192.168.42.124 6 use-vrf servers1

aaa accounting default group CiscoACS
```

Cisco Nexus switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco Nexus switches use NTP to meet these requirements by implementing the following configuration statements.

```
! NTP can only be configured in the default VDC
!
enable NTP
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management

clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
```

  To learn more about NTP, visit:
  http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Wireless

Cisco Wireless technologies provide connectivity for mobile clients within the branch. They can secure connectivity for traditional business functions such as guest access or inventory control, without increasing risk. Innovative customer experience services such as mobile point-of-sale are equally secure. In addition to expanding business functionality, Cisco wireless technology seamlessly provides the capability to detect rogues.

Industry-leading performance is available with Cisco Aironet access points for highly secure and reliable wireless connections for both indoor and outdoor environments. Cisco offers a broad portfolio of access points targeted to specific business needs and topologies.

Cisco wireless controllers help reduce the overall operational expenses of Cisco Unified Wireless Networks by simplifying network deployment, operations, and management. They extend the Cisco Borderless Network policy and security from the wired network to the wireless edge.

Cisco Wireless Control System (WCS) delivers full visibility and control of Cisco Aironet access points, Cisco Wireless LAN Controllers (WLC) and the Cisco Mobility Services Engine (MSE) with built-in support for Cisco adaptive wireless intrusion prevention systems (wIPS) and Cisco context-aware services. This robust platform helps you reduce total cost of ownership and maintain a business-ready wireless network.

Table 5-48 PCI Assessment Summary—Cisco Wireless Products

Models Assessed	
AIR-CT5508-12-K9 version 7.0.114.112 MSE3550 version 7.0.200.125 Cisco WCS Manager version 7.0.171.107 AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N	
PCI Sub-Requirements Passed	
PCI 2	2.1.1, 2.2, 2.2.2, 2.2.4, 2.3

Table 5-48 PCI Assessment Summary—Cisco Wireless Products (continued)

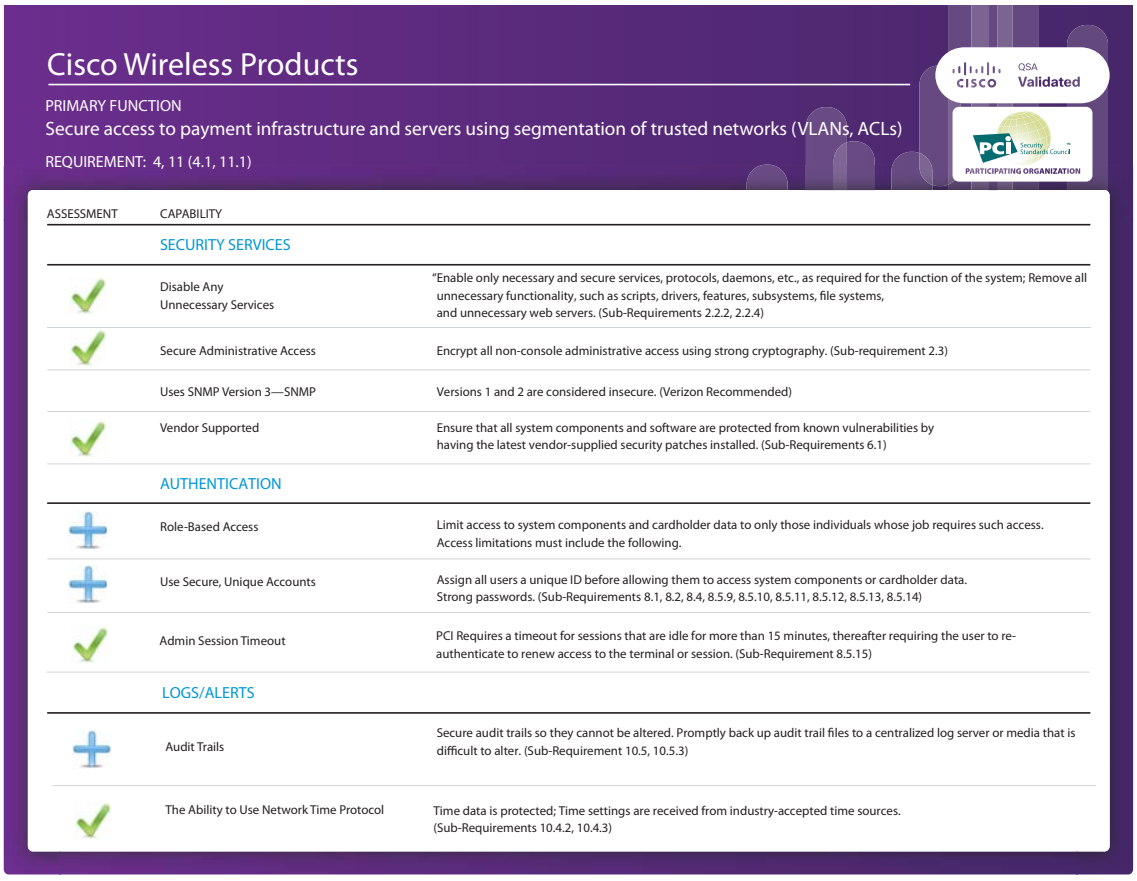
PCI 4	4.1, 4.1.1
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.1.b, 11.1.d
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary PCI function of Cisco Unified Wireless is secure connectivity of wireless clients (4.1) and rogue detection (1.1).

Table 5-49 lists the component assessment details for Cisco wireless products.

Table 5-49 Component Capability Assessment —Cisco Wireless Products



Cisco Wireless Products

PRIMARY FUNCTION

Secure access to payment infrastructure and servers using segmentation of trusted networks (VLANs, ACLs)

REQUIREMENT: 4, 11 (4.1, 11.1)

cisco QSA Validated

PCI Security Standards Council PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

Rogue detection for wireless technology in the branch is required at a minimum of once a quarter, whether or not the organization has wireless deployed. A hacker might infiltrate a branch and install a rogue wireless device (for example, access point, wireless-enabled printer, or radio-enabled USB stick). This would allow a hacker remote access into the branch (from the parking lot, for example) that is hard to detect. The PCI DSS offers several methods for detecting rogue devices. Cisco Unified Wireless offers the benefit of continuous rogue detection while simultaneously passing normal wireless traffic.

The PCI-DSS states that wireless technology is an untrusted network connection. Wireless technology in the branch requires firewall and intrusion detection services to segment and protect the cardholder data environment. Stateful firewalls must be configured to limit traffic to and from the wireless environment (all enabled services, protocols, and ports must have documented justification for business purposes). All other access must be denied.

When including point-of-sale clients in the wireless network, strong wireless encryption technology needs to be implemented.

Caution Wireless clients must be protected from each other, as well. For example, when using hand-held scanners and mobile POS, the scanners need to be on separate SSIDs and networks from the POS, and protected with firewall and intrusion detection services that are restricted to justified business access.

Wireless compliance is broken into the stages listed in Table 5-50.

Table 5-50 Wireless Compliance Stages

Wireless Deployment	Risk	Required Measure
No wireless deployed	Hacker deploys wireless into branch	Rogue detection
Wireless deployed, no wireless POS/CDE	Hacker deploys unknown wireless into branch, or hacks into existing wireless	Rogue detection Stateful firewall separating wired from wireless LAN Intrusion Detection System
Wireless deployed, includes wireless POS/CDE	Hacker deploys unknown wireless into branch, or hacks into existing wireless	Rogue detection Stateful firewall separating wired from wireless LAN Intrusion Detection System Strong wireless encryption for CDE (e.g., WPA2) Wireless CDE must be protected from other wireless and wired segments using a stateful firewall (Req. 1,2,3)

Cisco recommends using the Unified Wireless (controller-based) architecture for enterprise wireless deployments because of the Cisco ongoing wireless strategy. The autonomous Cisco IOS access points are not being enhanced. Future security and user enhancements will be developed on the controller-based architecture.

For WCS servers running software versions prior to 4.1, Cisco recommends a combination of documented password policies, manual audit procedures, and firewall segmentation for WCS servers within the data center.

- Configure unique SSIDs
- Disable broadcast of the SSIDs

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Whenever possible, a screenshot highlighting the appropriate Cisco Wireless Control System functionality is provided.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1.1**—*For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.*

  The Cisco Unified Wireless Network supports both Wi-Fi Protected Access (WPA) and WPA2 and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption (see Figure 5-113 and Figure 5-114). There is no default PSK, and all PSKs must be created during configuration. The Cisco Unified Wireless Network architecture does not use SNMP at the access points.

Figure 5-113 WLANs Security Screen

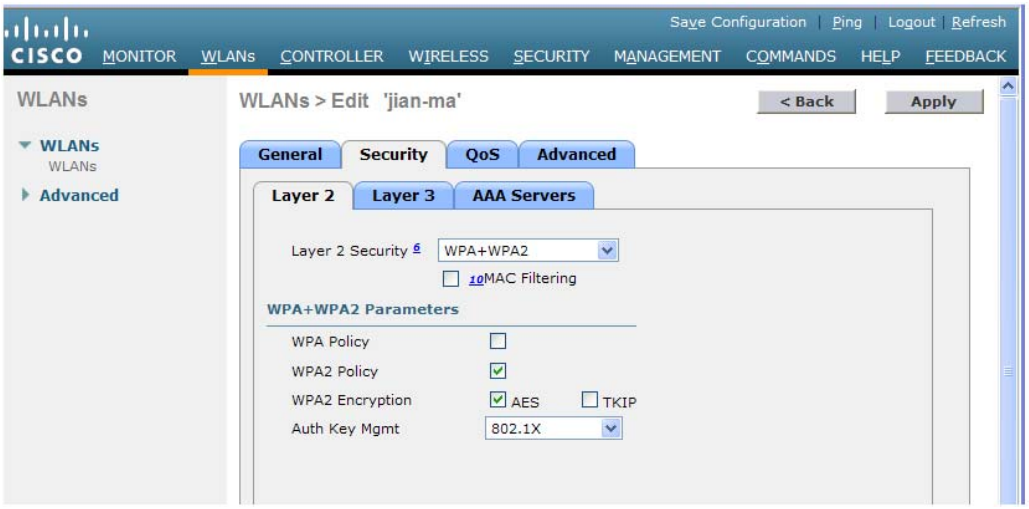
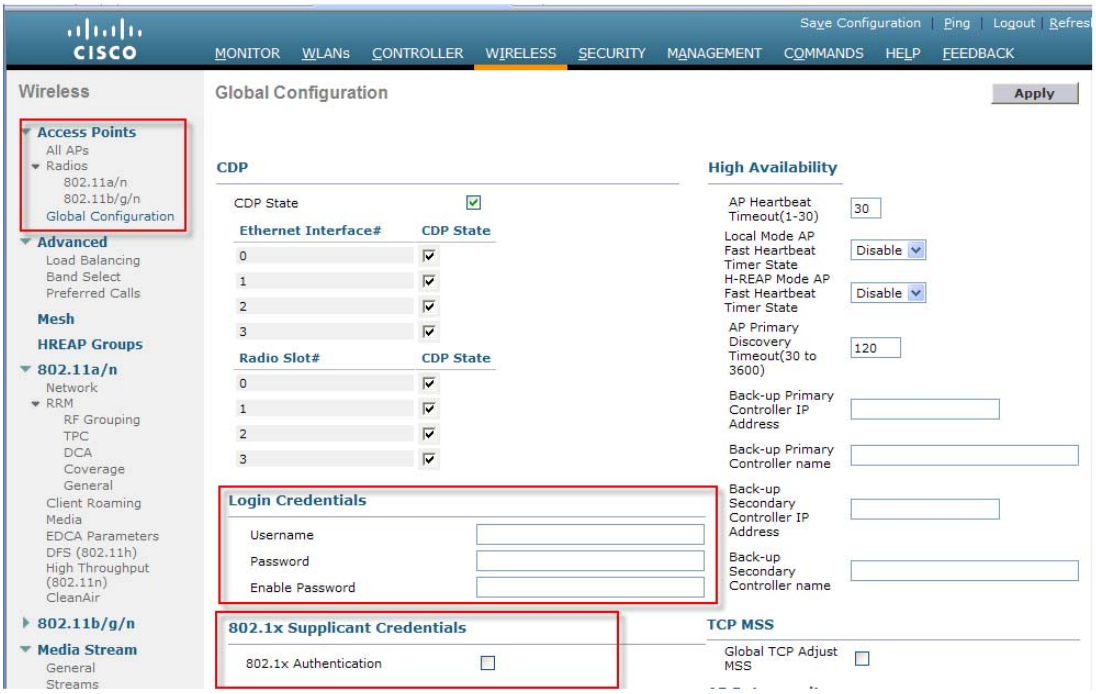


Figure 5-114 Wireless Global Configuration Screen



- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are no unnecessary services enabled by default on the Cisco Unified Wireless Control Server system. Cisco Unified Wireless Control Server should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository.

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers*

  Cisco Unified Wireless Control Server system should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

  Cisco Unified Wireless Control Server system can be configured for secure management using strong cryptography. Figure 5-115, Figure 5-116, Figure 5-117, and Figure 5-118 show where to disable non-encrypted management interfaces (for example, Telnet and HTTP).

Figure 5-115 WCS Server Secure Management

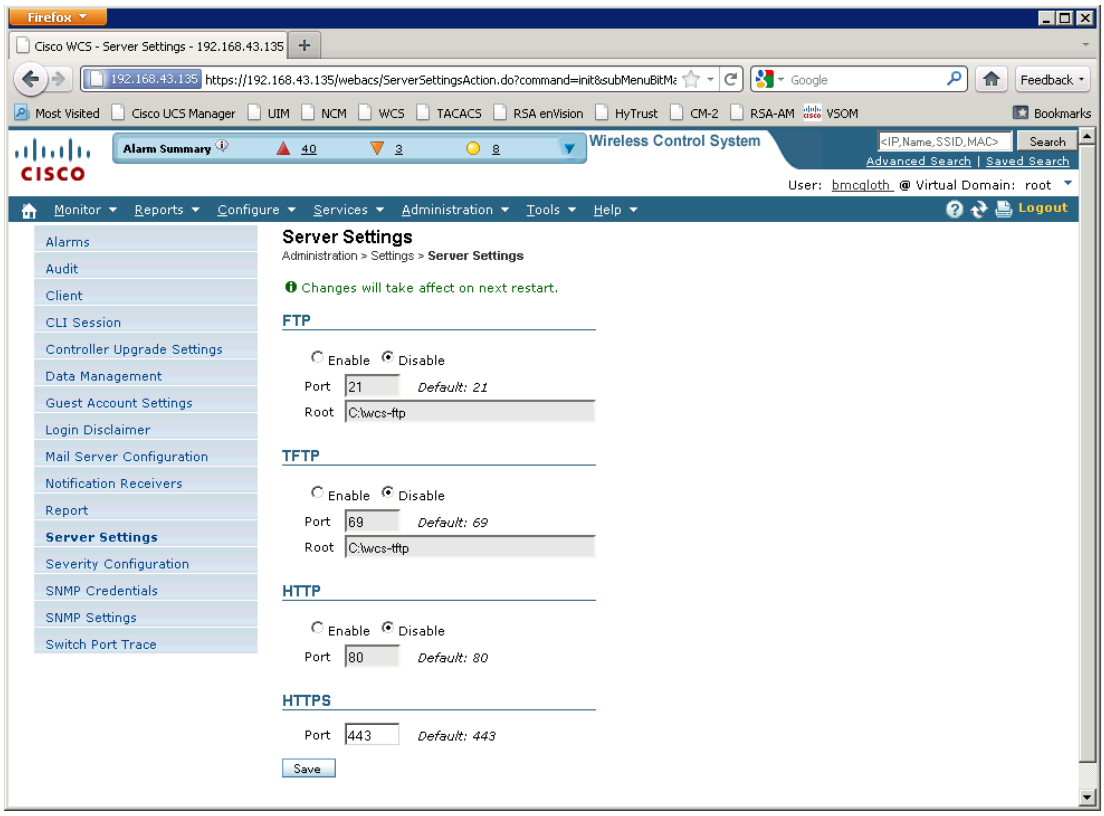


Figure 5-116 CLI Session Secure Management

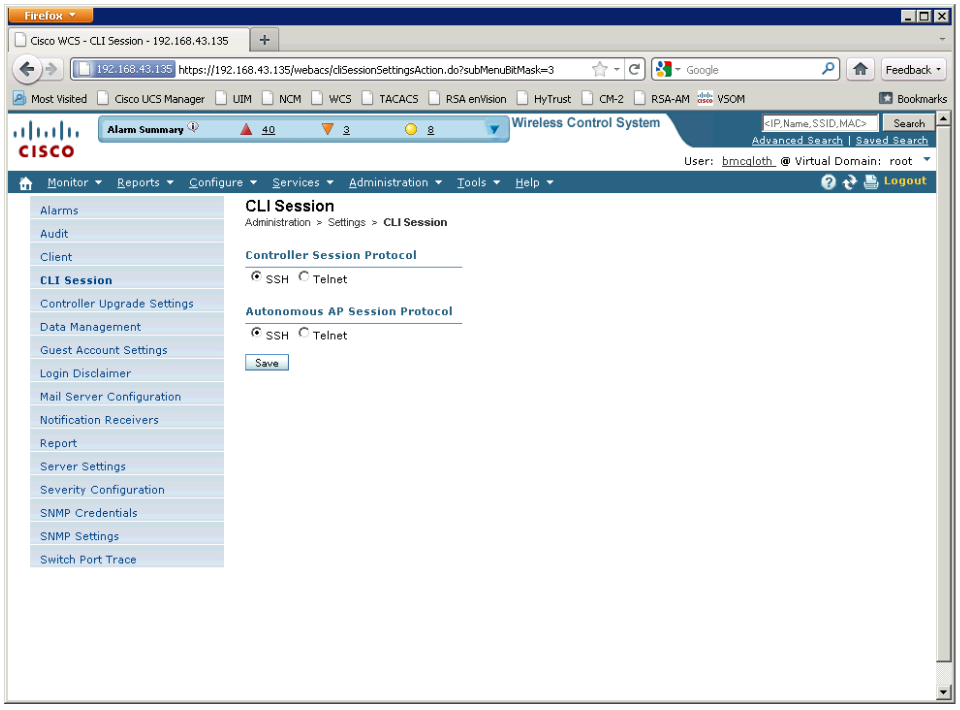


Figure 5-117 Controller Secure Management for SSH

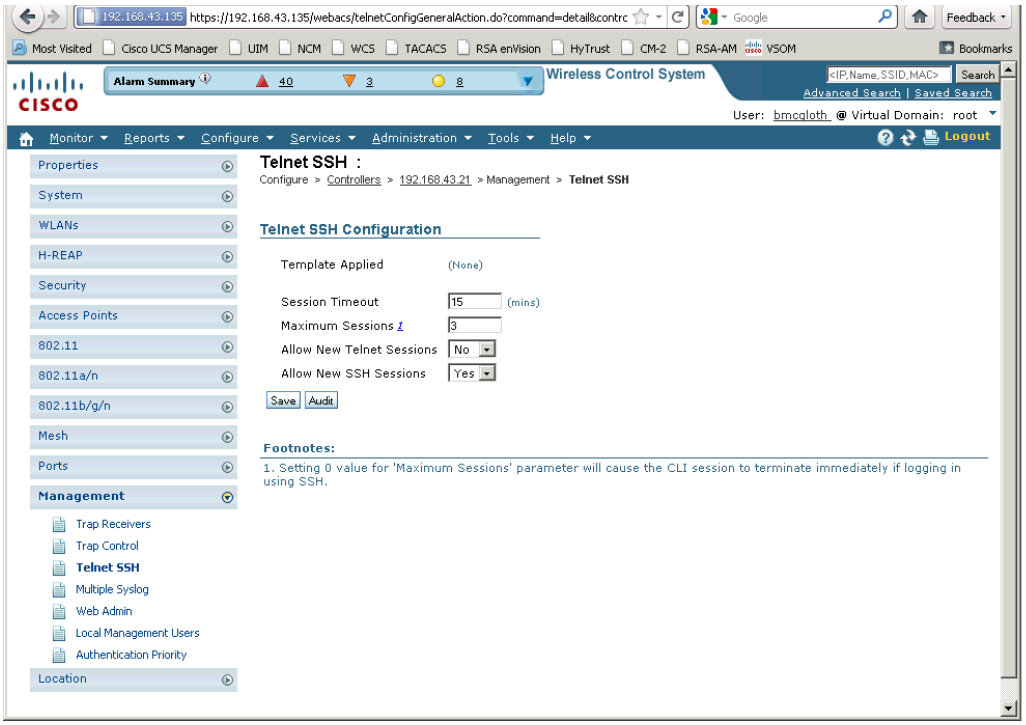
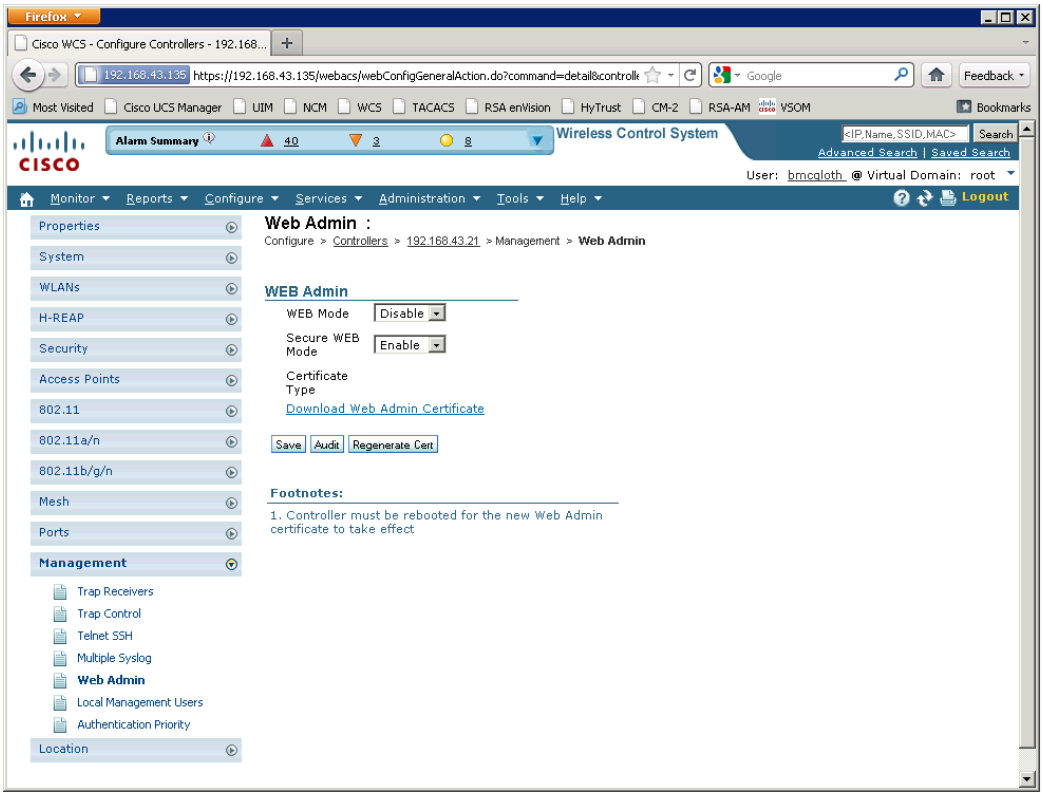


Figure 5-118 Controller Secure Management for HTTPS

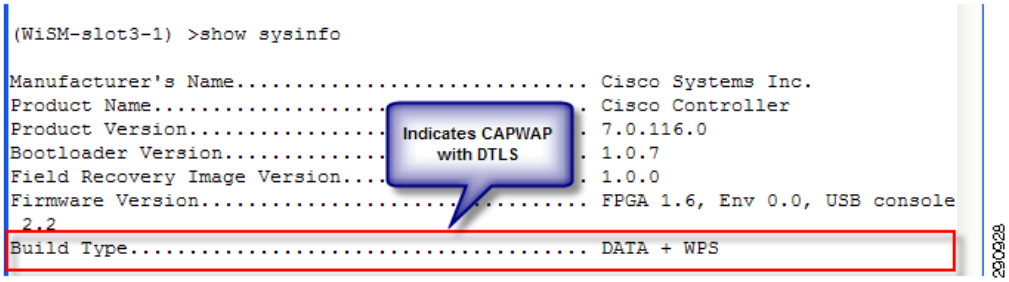


Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

  Cisco offers Control and Provisioning of Wireless Access Points (CAPWAP)-compliant DTLS encryption to ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links (see Figure 5-119). The Cisco Unified Wireless Network defaults to the highest CipherSuite available on the network. Furthermore, fallback on less secure SSL versions (that is, SSLv2 and SSLv1) can also be disabled, thus always forcing use of SSLv3. The Cisco Unified Wireless Network provides 256-bit encryption and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations.

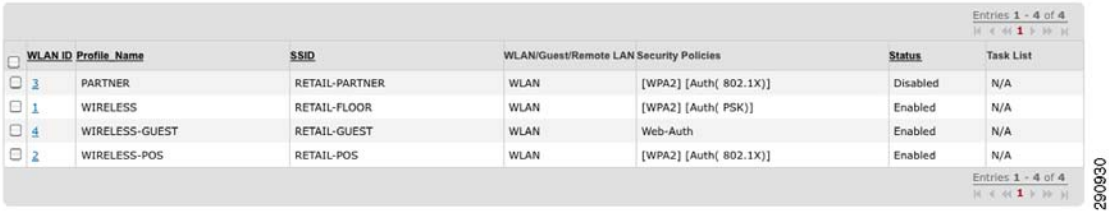
Figure 5-119 CAPWAP with DTLS



- **PCI 4.1.1**—*Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control was prohibited as of 30 June 2010.*

  Cisco supports both WPA and WPA2 and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption. Cisco does not advertise the organization's name in the Service Set ID (SSID) broadcast. Cisco also disables SSID broadcast by default for non-guest networks. Cisco supports WPA2 Personal mode with a minimum 13-character random pass-phrase and Advanced Encryption Standard (AES) encryption, and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations. (See Figure 5-120.)

Figure 5-120 WLAN Information



Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Unified Wireless. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

  For more information about PSIRT:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS using TACACS+ and RADIUS services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

Cisco Unified Wireless allows the network administrator to set user IDs that can be monitored and restricted with respect to access and other privileges when necessary.

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  The Cisco solution uses profiles where a user is assigned to the profile to ensure appropriate access to ensure network security, and user access can be restricted as shown in Figure 5-121 and Figure 5-122.

Figure 5-121 Local Management Users Screen

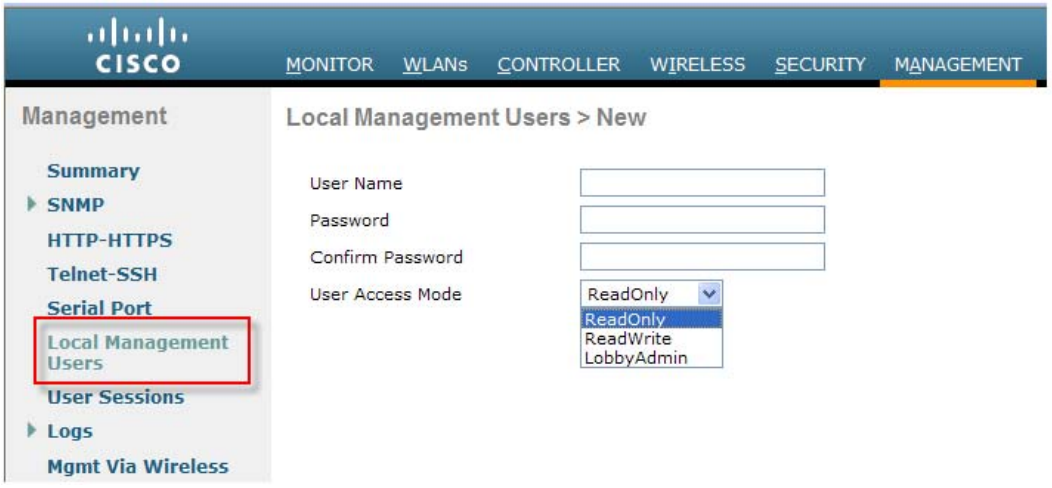
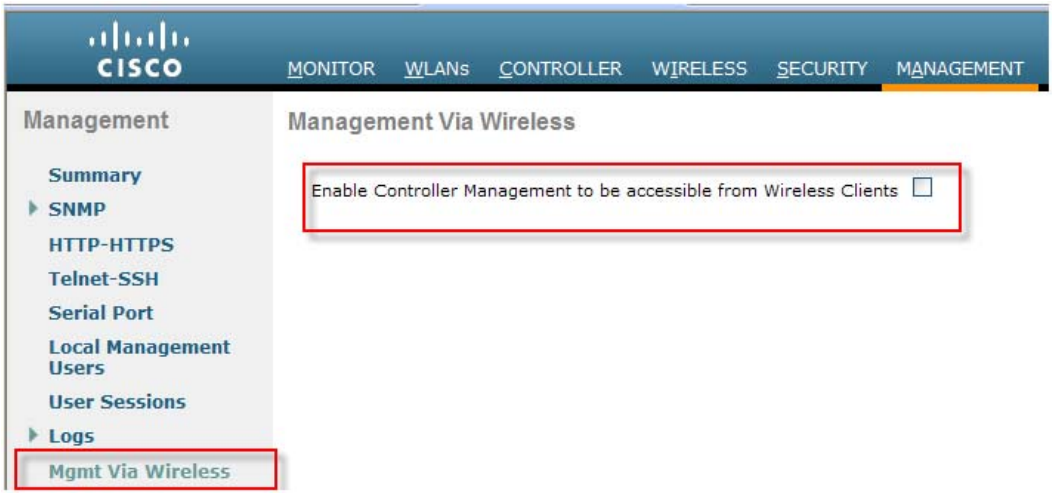
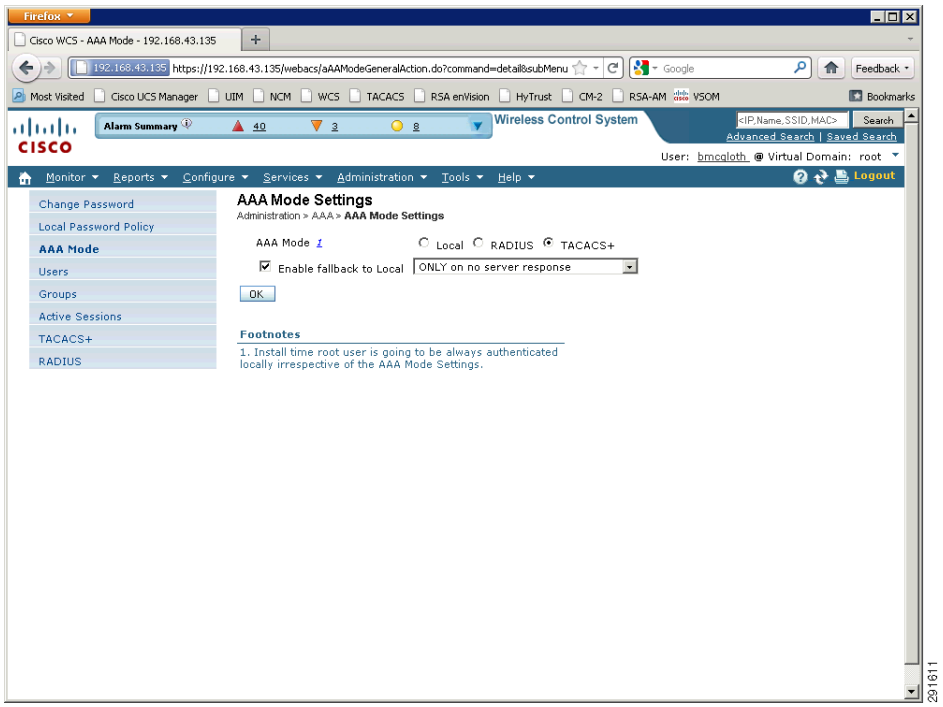


Figure 5-122 Management Via Wireless Screen



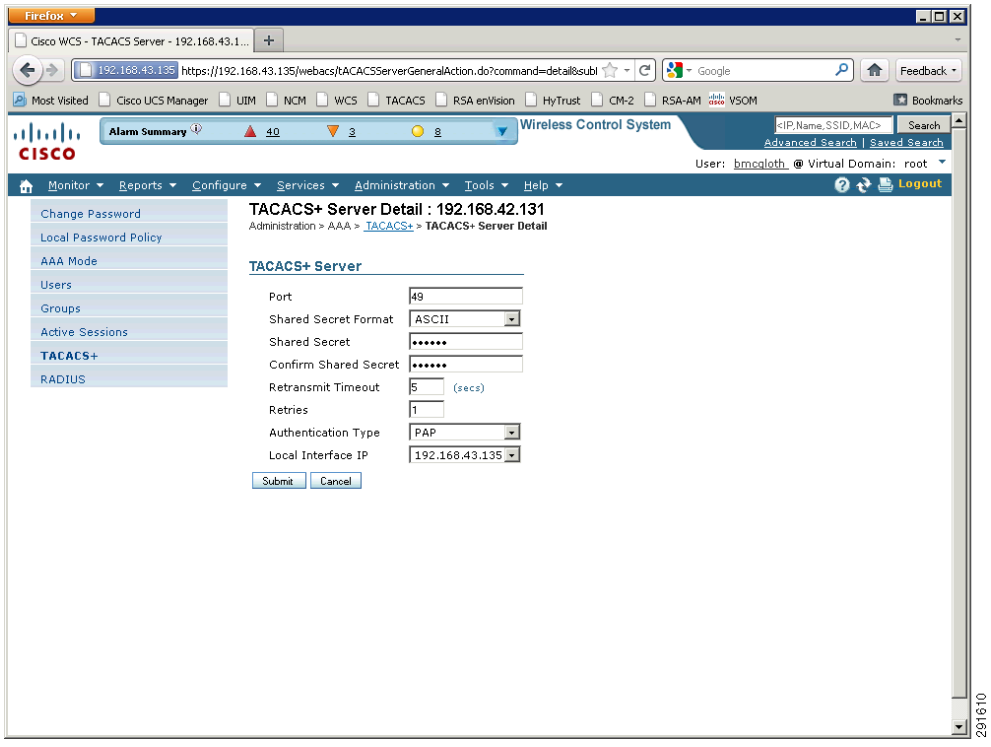
Cisco WCS is configured to use TACACS+ for authentication of administrators, as shown in Figure 5-123.

Figure 5-123 WCS Manager AAA Authentication Mode



The authentication servers for TACACS+ in WCS Manager are configured as shown in Figure 5-124.

Figure 5-124 WCS Manager TACACS+ Server Configuration



Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

Cisco Unified Wireless is able to meet some of the requirements locally, as identified below.

- **PCI 8.1**—Assign all users a unique ID before allowing them to access system components or cardholder data.

  Cisco WCS supports the creation of local user accounts with unique IDs. These can be used for local fallback user accounts. They should be individually unique as specified by policy.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco WCS Manager and controllers support the ability to specify a password.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Local user fall back accounts use MD5-encryption for the user password. Communication to the AAA server using RADIUS or TACACS+ is encrypted when using centralized authentication.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

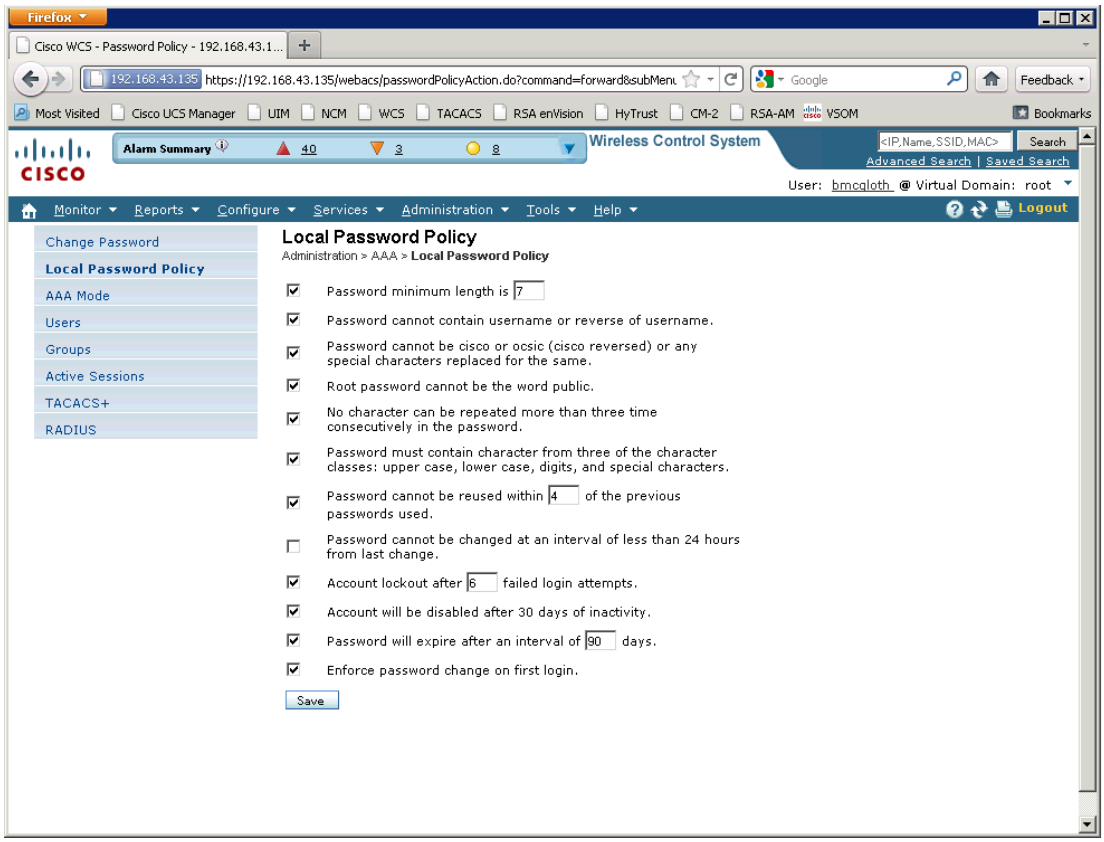
  Cisco Unified Wireless does not support an automated capability to perform this function at this time, user account would have to be manually reviewed in the device configurations every 90 days.

  The next several requirements (8.5.9–8.5.14) are addressed with the local password policy.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Figure 5-125 shows the local password policy that has been modified to meet the minimum requirements as specified by the preceding requirements.

Figure 5-125 WCS Manager Local Password Policy



- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to reactivate the terminal or session.*

  Cisco WCS Manager limits sessions, as shown in Figure 5-117 above.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco Unified Wireless system is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*

  Cisco Unified Wireless tracks individual administrator actions through several mechanisms including AAA, logging, and system events.

- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Figure 5-126 shows the configuration of local logging settings, and Figure 5-127 shows the syslog server configuration used to send logs to RSA enVision.

Figure 5-126 Local Logging Configuration

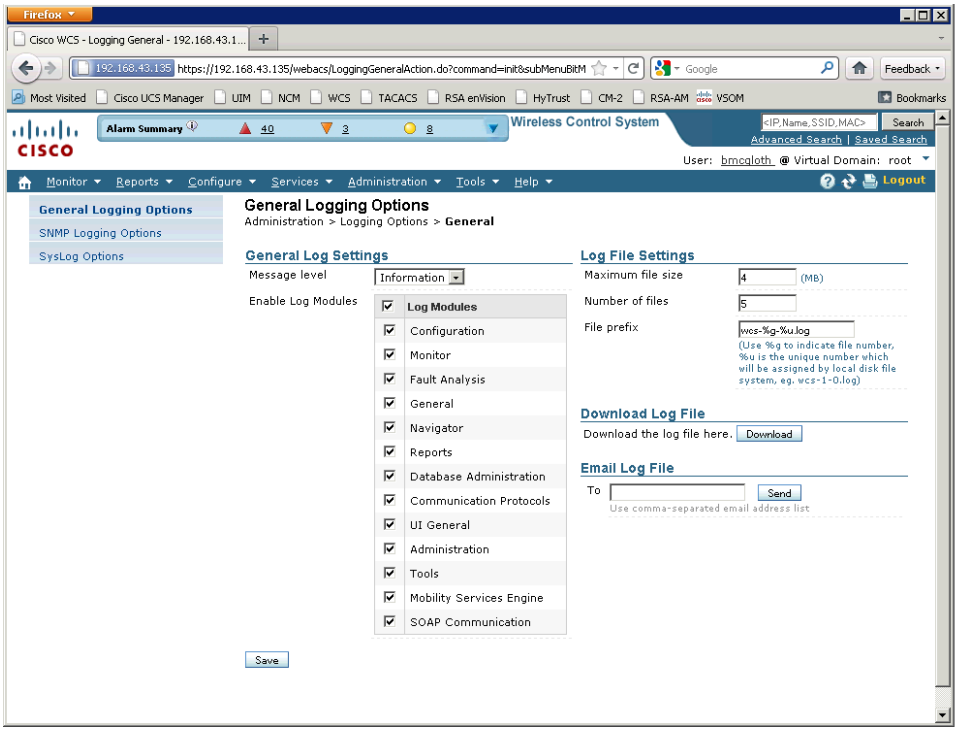
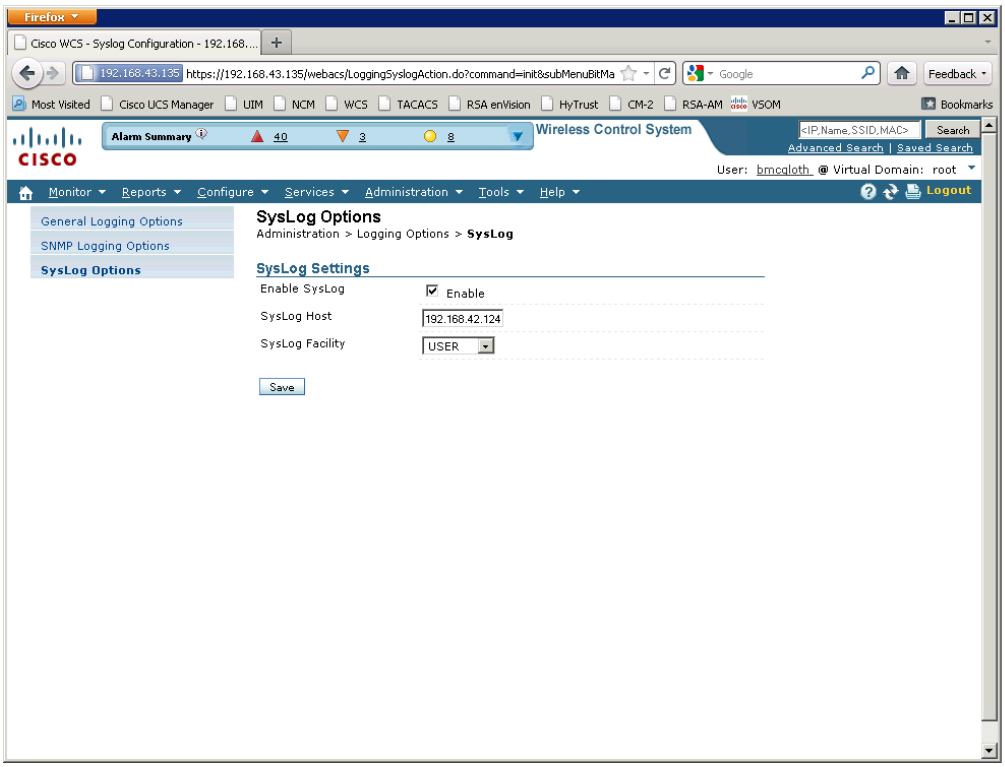


Figure 5-127 WCS Manager Syslog Configuration



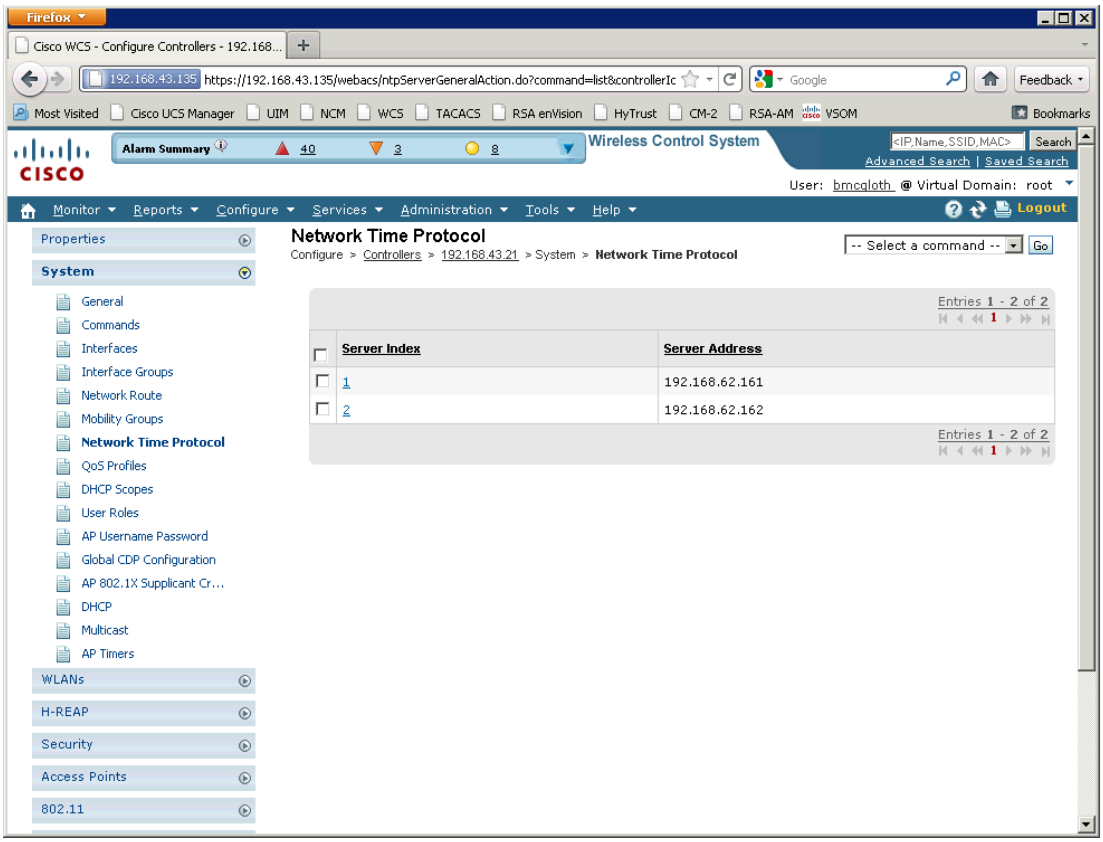
Cisco WCS uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

  A Network Time Protocol server can be configured within the Cisco WCS and Controllers to meet this requirement for all wireless devices, as shown in Figure 5-128.

Figure 5-128 NTP Servers Screen for Controllers



Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.1.b**—*Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:*
  - WLAN cards inserted into system components
  - Portable wireless devices connected to system components (for example, by USB, etc.)
  - Wireless devices attached to a network port or network device

  The Cisco WLAN performs 24-hour scanning to immediately detect and contain unauthorized and rogue wireless devices. Threats to network security can occur in between quarterly scans, creating the need to continuously scan and to use automatic alerts and containment mechanisms. Similarly, physical and/or port scanning on the wired network is not enough. Cisco Wireless LAN Controllers include wIPS and wIDS that find and stop rogue devices and attacks. WCS is a single point of management for WLAN devices, the mobility services engine, and mobility services. Cisco context-aware location services in the Cisco 3300 Series Mobility Services Engine (MSE) can locate

multiple rogue devices. Cisco enhanced local mode (ELM) access points offer monitor mode wIPS on local mode access points for additional protection without a separate overlay network. Cisco CleanAir technology allows the detection and location of rogue devices on nonstandard Wi-Fi channels. (See Figure 5-129 and Figure 5-130.)

Figure 5-129 Security—AP Policies Screen

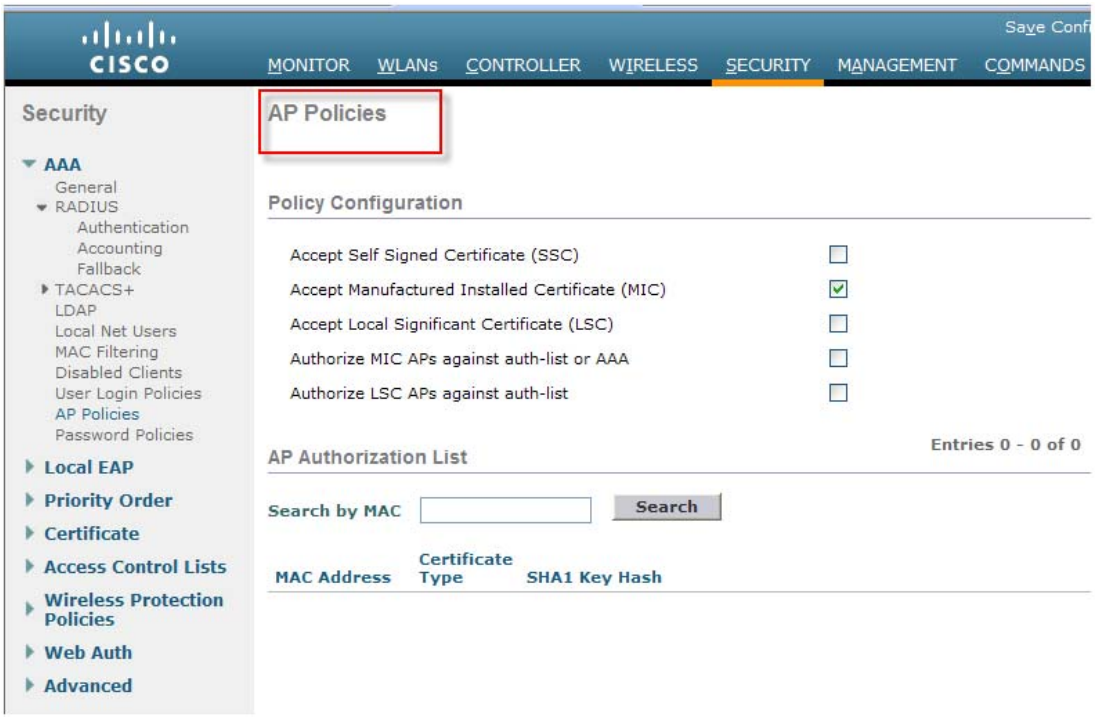
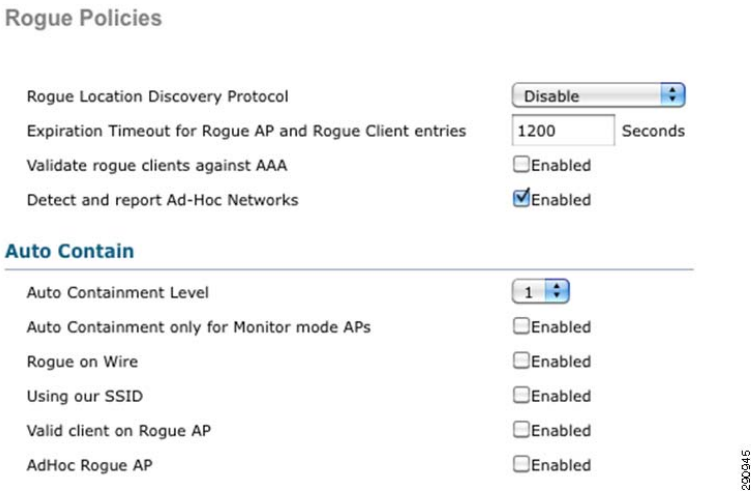


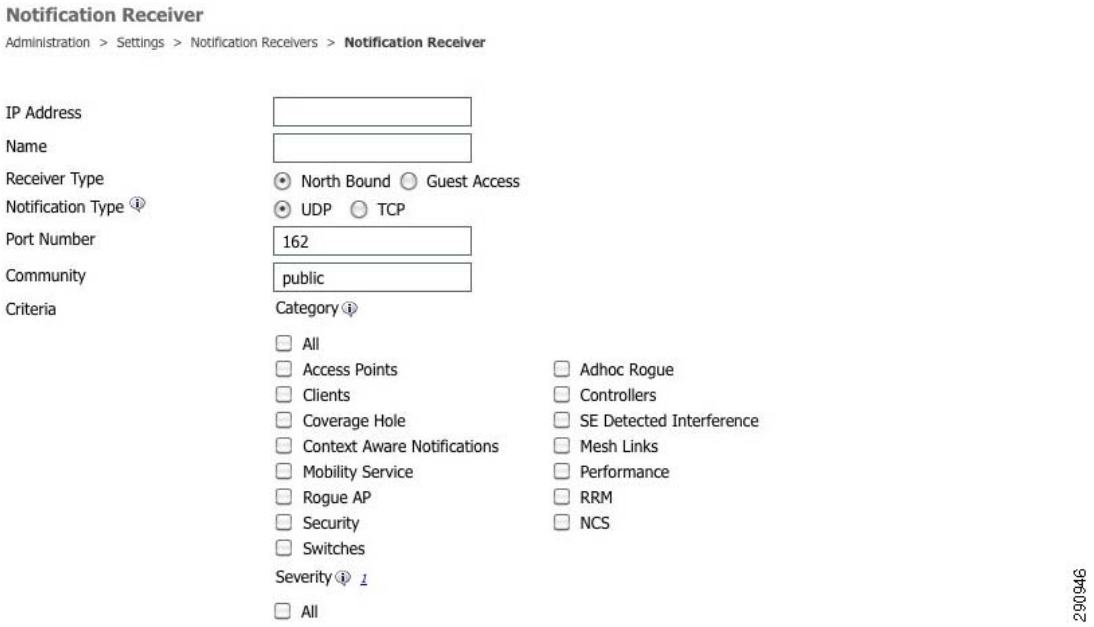
Figure 5-130 Rogue Policies Screen



- **PCI 11.1.d**—*If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.*

Cisco WCS has the ability to forward alerts to e-mail addresses. The system can forward all or selected alerts to multiple receivers. (See Figure 5-131.)

Figure 5-131 Notification Receiver Screen



PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Storage

Cisco MDS Storage Switches

Cisco MDS storage switches provide the central switching infrastructure connecting servers to storage. They provide the added capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.

The Cisco MDS 9000 Series Multilayer SAN Switches can help lower the total cost of ownership of the most demanding storage environments. By combining robust and flexible hardware architecture with multiple layers of network and storage management intelligence, the Cisco MDS 9000 Series helps you build highly available, scalable storage networks with advanced security and unified management.

Table 5-51 PCI Assessment Summary—Cisco MDS Storage Switches

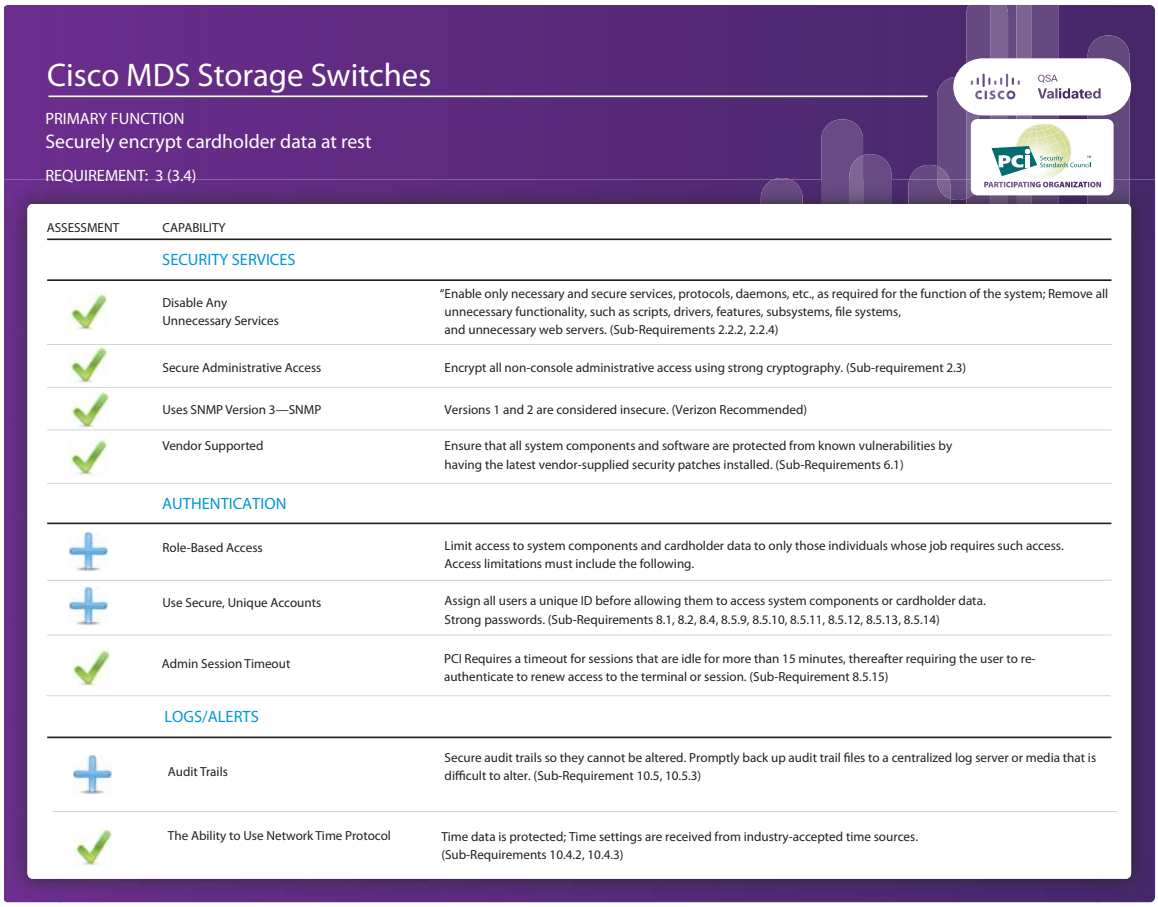
Models Assessed	
MDS 9506 (“Supervisor/Fabric-2”) version m9500-sf2ek9-mzg.5.0.1a.bin.S4 MDS 9506 (“Supervisor/Fabric-2”) version m9500-sf2ek9-mz.5.0.4.bin	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 3	3.4.1, 3.5, 3.5.1, 3.5.2, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of Cisco MDS storage switches is to securely encrypt cardholder data at rest as it passes from server to storage. (3.4)

Table 5-52 lists the component assessment details for Cisco MDS storage switches.

Table 5-52 Component Capability Assessment—Cisco MDS Storage Switches



Cisco MDS Storage Switches

PRIMARY FUNCTION
Securely encrypt cardholder data at rest

REQUIREMENT: 3 (3.4)

cisco QSA Validated

PCI Security Standards Council PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

The MDS 9500s were configured for zoning and LUN masking to secure the logical partitioning of disk used for storing cardholder data. Only host machines in the data center that require access to that logical disk partition were allowed access. Configuration of the VSANs, host UUIDs, and mappings was partially performed using EMC Unified Infrastructure Manager as directed by the Vblock architecture by VCE. Vblock requires specific software versions and pre-configurations to be completed as specified in the Vblock preparation guide.

More information of Vblock designs can be found at the following URL:
http://www.vceportal.com/solutions/68580567.html#

Information in installing and configuring Cisco MDS can be found at the following URL:
http://www.cisco.com/en/US/products/hw/ps4159/ps4358/tsd_products_support_series_home.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

The Cisco MDS 9000 NX-OS Software does not use defaults for system passwords and other security parameters, but instead prompts the user for this information at power-up and can enforce the use of PCI-compliant passwords.

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are two ways to do this: initial setup, or configuration after the fact.

  1. Initial setup

```
 ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
Do you want to enforce secure password standard (yes/no) [y]: yes
Create another login account (yes/no) [n]:
Configure read-only SNMP community string (yes/no) [n]: yes
Configure read-write SNMP community string (yes/no) [n]: yes
Enter the switch name :
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
Mgmt0 IPv4 address :
Configure the default gateway? (yes/no) [y]:
IPv4 address of the default gateway :
Configure advanced IP options? (yes/no) [n]:
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) [rsa]:
Number of rsa key bits <768-2048> [1024]:
Enable the telnet service? (yes/no) [n]: no
Enable the http-server? (yes/no) [y]: no
Configure clock? (yes/no) [n]:
Configure timezone? (yes/no) [n]:
Configure summertime? (yes/no) [n]:
Configure the ntp server? (yes/no) [n]: yes
Configure default switchport interface state (shut/noshut) [shut]: shut
Configure default switchport trunk mode (on/off/auto) [on]:
Configure default switchport port mode F (yes/no) [n]: yes
Configure default zone policy (permit/deny) [deny]: deny
Enable full zoneset distribution? (yes/no) [n]:
Configure default zone mode (basic/enhanced) [basic]:
```

  2. By configuration after the fact

```
Configure terminal
Password strength-check
snmp-server community <password> ro
snmp-server community <password> rw
feature ssh
ssh key dsa or ssh key rsa <768-2048>
no feature telnet
no feature http-server
ntp server <ip address>
system default switchport shutdown
system default switchport mode f
no system default zone default-zone permit
```

  3. Additional

```
Secure access to management port:
ip access-list 23 permit ip 127.0.0.1 0.0.0.0 <mgmt port ip address> 0.0.0.0
ip access-list 23 permit ip <ip address of mgmt workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of snmp workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of AAA server> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of NTP workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 deny ip any any log-deny
interface mgmt0
ip address <ip address> <mask>
ip access-group 23 in
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco MDS switch is a hardened device that does not allow changes to the operating system.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The Cisco MDS switch uses SSL for web-based administrative and user access, and uses SSH for remote terminal access by implementing the configurations shown above.

Requirement 3: Protect Stored Cardholder Data

Cisco Storage Media Encryption (SME) provides protection of cardholder data by delivering disk and tape encryption. Cisco SME stores the keys in the Cisco key management server or in a secure third-party key manager such as RSA KM.

- **PCI 3.4.1**—*If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.*

  Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.

  The SME feature of the Cisco MDS 9000 SAN fabric is independent of the native operating system access control. Decryption keys are managed by the Cisco Key Manager, which is part of the SME feature. Keys are tied to individual tapes or LUNs, not to user accounts.

- **PCI 3.5**—*Protect any keys used to secure cardholder data against disclosure and misuse. Note: This requirement also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*

  All keys are stored in encrypted form, and are always encrypted for transmission within the fabric.

- **PCI 3.5.1**—*Restrict access to cryptographic keys to the fewest number of custodians necessary.*

  Only recovery officers have access to the master key, stored in the PIN-protected smart cards. Only the key administrators have access to the disk and tape keys, stored in encrypted format in the Cisco Key Manager Center (KMC) or the RSA key manager.

- **PCI 3.5.2**—*Store cryptographic keys securely in the fewest possible locations and forms.*

Keys are stored in encrypted form in Cisco Key Manager, or stored by Cisco Key Manager in the RSA Key Manager. Both key managers provide for secure backup and recovery of keys, and for their secure storage in an alternate location. The master key is spread across multiple smart cards, each protected by a PIN chosen by the depository recovery officer.

- **PCI 3.6.1**—*Generation of strong cryptographic keys*

  The cryptographic keys (AES 256 bits) are generated by the encryption engine within the services node.

- **PCI 3.6.2**—*Secure cryptographic key distribution*

  The keys are never transmitted in clear text, but always using secure protocols (HTTPS and SSL).

- **PCI 3.6.3**—*Secure cryptographic key storage*

  Key-encrypting keys are stored in encrypted format in the Cisco KMC. Master keys are stored in PIN-encrypted format in the smart cards.

- **PCI 3.6.4**—*Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of ciphertext has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).*

  Cisco SME offers the capability to re-key and change keys as needed. Customers must enforce and document this procedure appropriately.

- **PCI 3.6.5**—*Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*

  Cisco KMC can manage the complete key lifecycle. Customers need to implement and document this procedure appropriately.

Requirement 6: Develop and Maintain Secure Systems and Applications

Cisco MDS 9000 NX-OS provides the capability to use a test VSAN to validate any new configuration before production. Cisco MDS 9000 NX-OS has also been developed with secure coding guidelines and is tested against common vulnerabilities.

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco MDS switches. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

Cisco MDS 9000 Family security features such as VSANs, advanced zoning, fabric binding, port security, Fibre Channel Security Protocol (FC-SP) authentication, and role-based access control (RBAC) with SNMPv3 and SSH make the Cisco MDS 9000 Family an excellent platform for enforcing this requirement. SSH RBAC in particular, if used in conjunction with VSANs, is especially designed to support tight partitioning of the physical infrastructure.

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS using TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- This is accomplished using the user role feature (see 7.2.2).
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- This is accomplished using the user role feature (see 7.2.2).
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

The following configurations demonstrate how to configure the Cisco MDS for TACACS+ authentication to a central server.

```
Feature tacacs+

tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131

aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable
```

Note To configure LDAP authentication in NX-OS version 5.0 or higher, enable LDAP (**feature ldap**) and follow configuration steps in the Cisco MDS 9000 Family NX-OS Security Configuration Guide.

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*

```
Feature privilege
    change admin user ID:
    username admin password <password> role network-admin (password will be
encrypted when displayed)
    create network operator type user ID:
    username <assigned name> password <password> role network-operator (password
will be encrypted when displayed)
```

```
    create default user ID:
    role name default-role
        description This is a system defined role and applies to all users.
        rule 5 permit show feature environment
        rule 4 permit show feature hardware
        rule 3 permit show feature module
        rule 2 permit show feature snmp
        rule 1 permit show feature system
    username <assigned name> password <password> role default-role (password will
be encrypted when displayed)
    create custom user ID:
    role name <name>
        description User defined permissions define here:
        rule 1 permit show interface
        .
        .
        Rune 256 permit show module
    username <assigned name> password <password> role <name> (password will be
encrypted when displayed)
```

- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  All user access is controlled by the user role function; there is no generic user access.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

The Cisco MDS 9000 Family provides the capability to create an individual account for each administrator with a strong password. Authentication can be performed using the external authentication, authorization, and accounting (AAA) server of choice (for example, TACACS+) to implement the desired user authentication and password management policies.

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  To enforce session lengths, enable this using **terminal session-timeout** <*time in minutes*>.

```
line vty
  exec-timeout 15
line console
  exec-timeout 15
```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco MDS 9000 Family implements the Cisco Data Center Network Manager (DCNM), which continuously monitors the SAN and allows you to establish criteria and thresholds to generate real-time alarms and call-home functions. Syslog offers detailed entries and can be redirected to a log server to consolidate IT infrastructure monitoring information. Note that the log never contains application data.

Cisco MDS is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco MDS uses the local clock facilities to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco MDS use NTP to meet these requirements by implementing the following configuration statements:

```
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
ntp server 192.168.62.161
ntp server 192.168.62.162
```

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco MDS is capable of sending system events to a centralized repository using the syslog function and SNMP traps. Logs stored locally are buffered and require operator level privileges on the router to be viewed. External logging and SNMP traps are enabled by implementing the following configuration statements:

  ```
  logging server 192.168.42.124 6
  ```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Security

Cisco ASA 5500 Series—Branch

The Cisco ASA 5500 Series Adaptive Security Appliances provide secure segmentation within the branch. Their stateful firewall and modular intrusion detection modules enable the branch to securely connect public networks to the cardholder data environment.

The Cisco ASA 5500 Series delivers superior scalability, a broad span of technology and solutions, and effective, always-on security designed to meet the needs of a wide array of deployments. By integrating the world's most proven firewall; a comprehensive, highly effective intrusion prevention system (IPS) with Cisco Global Correlation and guaranteed coverage; high-performance VPN and always-on remote access, the Cisco ASA 5500 Series helps organizations provide secure, high performance connectivity and protects critical assets for maximum productivity.

The Cisco ASA 5500 Series includes the Cisco ASA 5505, 5510, 5512-X, 5515-X, 5520, 5525-X, 5540, 5545-X, 5550, 5555-X, 5580, and 5585-X Adaptive Security Appliances-purpose-built, high-performance security solutions that take advantage of Cisco expertise in developing industry-leading, award-winning security and VPN solutions. Through Cisco Multi-Processor Forwarding (MPF), the Cisco ASA 5500 Series brings a new level of security and policy control to applications and networks. MPF enables highly customizable, flow-specific security policies that have

been tailored to application requirements. The performance and extensibility of the Cisco ASA 5500 Series is enhanced through user-installable security service modules (SSMs) and virtual modules. This adaptable architecture enables businesses to rapidly deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and content security services such as those delivered by the Adaptive Inspection and Prevention (AIP) and Content Security and Control (CSC) SSMs. Furthermore, the modular hardware architecture of the Cisco ASA 5500 Series, along with the powerful MPF, provides the flexibility to meet future network and security requirements, extending the outstanding investment protection provided by the Cisco ASA 5500 Series and allowing businesses to adapt their network defenses to new threats as they arise.

All Cisco ASA 5500 Series appliances offer both IPsec and SSL/DTLS VPN solutions; clientless and AnyConnect VPN features are licensed at various price points, on a per-seat and per-feature basis. By converging SSL and IPsec VPN services with comprehensive threat defense technologies, the Cisco ASA 5500 Series provides highly customizable, granular network access tailored to meet the requirements of diverse deployment environments, while providing advanced endpoint and network-level security.

Table 5-53 PCI Assessment Summary—Cisco ASA 5500 Series (Branch)

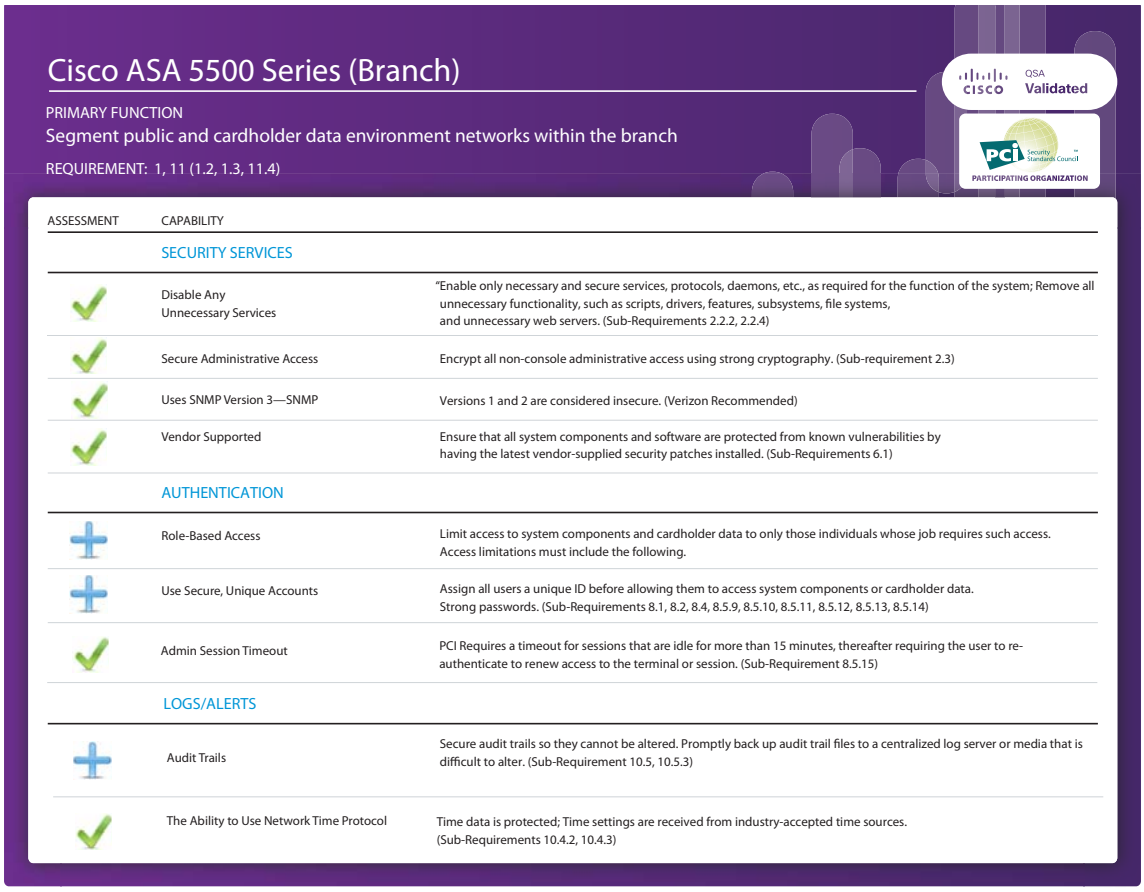
Models Assessed	
Cisco ASA5515-X w/vIPS Module version asa900-129-smp-k8.bin and IDS version 7.1(6)	
PCI Sub-Requirements Passed	
PCI 1	1.2.1, 1.2.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 4	4.1
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.4
PCI 11	11.4
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of the branch Cisco ASA firewall is to securely segment public and cardholder data environment branch networks, and provide intrusion detection capabilities. (1.2, 1.3, 11.4)

Table 5-54 lists the component assessment details for the Cisco ASA 5500 Series.

Table 5-54 Component Capability Assessment—Cisco ASA 5500 Series (Branch)



Cisco ASA 5500 Series (Branch)

PRIMARY FUNCTION
Segment public and cardholder data environment networks within the branch

REQUIREMENT: 1, 11 (1.2, 1.3, 11.4)

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Select the appropriate Cisco ASA model and IPS module for the traffic needs in the branch.
- For ASAs with SSM modules, connect the external Ethernet interface of the module to the secure management segment of the branch network.
- Configure security policies, objects, and rules centrally with Cisco Security Manager.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco ASA firewalls are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted.

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Firewall configuration files are backed up centrally using Cisco Prime LMS. These tools also verify that running and startup configurations of firewalls, routers, and switches are synchronized. Additionally, Cisco Security Manager stores a copy of the firewall configuration for the policies that it manages.

- **PCI 1.2.3**—*Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.*
- **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*
- **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

The following configuration example shows how objects identify hosts and services within the network and their use in an access list to permit approved traffic:

```
!
interface Ethernet0/0
 nameif MSP-WAN
 security-level 0
 ip address 10.10.255.176 255.255.255.0
!
interface Ethernet0/1.1000
 vlan 1000
 nameif MANAGEMENT
 security-level 100
 ip address 10.10.191.1 255.255.255.0
!
! ----Defining Objects and Object Groups----
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 network-object 192.168.42.122 255.255.255.255
object-group network CSManager
 description Cisco Security Manager
 network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
 network-object 192.168.42.138 255.255.255.255
object-group network POS-Store-MSP
 network-object 10.10.176.81 255.255.255.255
!
object-group service CSM_INLINE_svc_rule_73014461184
 description Generated by CS-Manager from service of FirewallRule# 4
(ASA-Store_V2/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object object ORACLE-OAS
 service-object object TOMAX-8990
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
```

```
 group-object ORACLE-WAS
 group-object HTTPS-8443
!
object-group network CSM_INLINE_src_rule_73014461184
 description Generated by CS-Manager from src of FirewallRule# 4
(ASA-Store_V2/mandatory)
 group-object DC-POS-Tomax
 network-object object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
! ----One line of the larger access-list permitting traffic----
!
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461184
object-group CSM_INLINE_src_rule_73014461184 object-group POS-Store-MSP
!
! ----Applying the access-list to an interface----
!
access-group OUTSIDE in interface MSP-WAN
```

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco ASA firewalls allow only administrative connections from authorized hosts/networks, as specified in the device configuration. The HTTP server supports only secure connections using SSL. If no hosts or networks are specified for the service, it is effectively disabled (for example, the Telnet service). The following configuration shows the authorized management hosts for SSH and HTTPS administration, and none for Telnet.

```
http server enable
http 192.168.41.101 255.255.255.255 MSP-WAN
http 192.168.41.102 255.255.255.255 MSP-WAN
http 192.168.42.122 255.255.255.255 MSP-WAN
http 192.168.42.124 255.255.255.255 MSP-WAN
http 192.168.42.133 255.255.255.255 MSP-WAN
http 192.168.42.138 255.255.255.255 MSP-WAN
telnet timeout 5
ssh 192.168.41.101 255.255.255.255 MSP-WAN
ssh 192.168.41.102 255.255.255.255 MSP-WAN
ssh 192.168.42.122 255.255.255.255 MSP-WAN
ssh 192.168.42.124 255.255.255.255 MSP-WAN
ssh 192.168.42.133 255.255.255.255 MSP-WAN
ssh 192.168.42.138 255.255.255.255 MSP-WAN
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco ASA firewalls do not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco ASA firewalls support strong encryption for SSH and HTTPS. The following configurations are used to configure strong cryptography:

```
! ---Specify only Strong algorithms for SSL connections---
!
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1
!
! ---Specify strong encryption version of SSH
!
ssh version 2
!
```

SNMP versions 1 and 2(c) transmit data between the SNMP server and the SNMP agent "in the clear". This makes your infrastructure and corresponding infrastructure devices vulnerable to attack and or misuse. SNMP v3 adds authentication and privacy options to secure its communication between SNMP servers and SNMP agents.

Cisco ASA firewalls allow secure administration using SNMP version 3 with encryption and authentication using the "priv" security model.

SNMP groups provide an access control policy to which users are added. The user inherits the security model of the group.

SNMP users are assigned a username, a group to which they belong, authentication password, encryption password, and associated algorithms to use. Authentication algorithms are MD5 and SHA. Encryption algorithms are DES, 3DES, and AES (128,192,256).

```
snmp-server enable
snmp-server group V3Group v3 priv
snmp-server user ciscolms V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
snmp-server user csmadmin V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
```

An SNMP host is the server to which SNMP notifications and traps are sent. SNMP v3 hosts require the SNMP server IP address and SNMP username. Each SNMP host can have only one username associated with it. The user credentials on the NMS (CiscoPrime, EMC NCM, and so on) must match the SNMP username credentials.

```
snmp-server host MSP-WAN 192.168.42.134 version 3 ciscolms
snmp-server host MSP-WAN 192.168.42.139 version 3 ciscolms
snmp-server host MSP-WAN 192.168.42.133 version 3 csmadmin
```

Enable the SNMP traps (this will change depending on environment and business requirements). The following example enables all, but this could be limited to a subset of traps.

```
snmp-server enable traps all
snmp-server location Building SJC-17-1 Aisle 1 Rack 3
snmp-server contact EmployeeA
```

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco ASA Firewalls. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

  For more information about PSIRT:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS using TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco ASAs are configured to use a AAA model for user-based access. Users can be assigned to groups and, based on privilege levels, have access to only the information they require for their job function. By default in Cisco ASA, no users are allowed access unless specifically configured and assigned appropriate passwords.

```
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (MANAGEMENT) host 192.168.42.131
 key <removed>
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
```

  Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa authentication ssh console RETAIL LOCAL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

The Cisco ASA is able to meet some of the requirements locally, as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco ASA supports the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username csmadmin password <removed> encrypted privilege 15
  username retail password <removed> encrypted privilege 15
  username bmcgloth password <removed> encrypted privilege 15
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco ASA require setting of a password.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of strong MD5-encrypted hashing of locally stored passwords, Cisco ASA also supports the use of AES encryption of pre-shared keys.

  ```
  password encryption aes
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco ASAs do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Security Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco ASA does not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Security Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco ASA does not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco ASA does not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco ASA does not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

  PCI 8.5.13—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco ASA management interfaces are configured as follows to meet this requirement:

```
http server idle-timeout 15
ssh timeout 15
```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco ASA 5500 is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco ASA uses the local clock facilities meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco ASA use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.162 source MSP-WAN
ntp server 192.168.62.161 source MSP-WAN prefer
clock timezone PST -8
clock summer-time PDT recurring
```

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.4**—*Write logs for external-facing technologies onto a log server on the internal LAN.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco ASA is capable of sending system events to a centralized repository using the syslog function and SNMP traps. Logs stored locally are buffered and require operator level privileges on the router to be viewed. External logging and SNMP traps are enabled by implementing the following configuration statements:

```
logging enable
logging timestamp
logging trap informational
logging asdm informational
logging host MSP-WAN 192.168.42.124
```

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4**—*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco ASA 5500 Series—Data Center

As a core component of Cisco Borderless Networks, Cisco ASA 5500 Series Adaptive Security Appliances provide:

- Context-aware firewall capabilities
- Proven firewall services
- Comprehensive real-time threat defense
- Effective, always-on, highly secure remote access
- Highly secure communication services

These solutions help reduce deployment and operational costs while delivering comprehensive network security for networks of all sizes.

Context-aware firewalling capabilities combine:

- In-depth local network context from Cisco ISE
- Real-time global threat intelligence from Cisco Security Intelligence Operations (SIO)
- Unique mobile client insight from AnyConnect

In addition, these solutions offer an advanced intrusion prevention system (IPS) with Global Correlation, which is twice as effective as a traditional IPS and includes Cisco guaranteed coverage.

Table 5-55 PCI Assessment Summary—Cisco ASA 5500 Series (Data Center)

Models Assessed	
Cisco ASA5555-X w/vIPS module version asa900-129-smp-k8.bin and IPS version 7.1(6)E4 Cisco ASA5585-S60-2A-K9 asa901-smp-k8.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.1, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 4	4.1
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.3, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.4
PCI 11	11.4
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary functions of the data center firewalls are twofold. They operate as a firewall, restricting traffic between the cardholder data environment and other areas of the network; and they operate as an intrusion prevention system, inspecting all traffic going to and from the cardholder data environment. These controls map directly to satisfying a number of PCI sub-requirements including Requirements 1, 2, 4, 7, 8, 10, and 11. The following is a description of how each of the PCI sub-requirements is satisfied for branch routers.

Table 5-56 lists the component assessment details for Cisco ASA 5500 Series.

Table 5-56 Component Capability Assessment —Cisco ASA 5500 Series (Data Center)

Cisco ASA 5500 Series (Data Center)

PRIMARY FUNCTION
Restrict traffic between the cardholder data environment and other network areas, and as an IPS

REQUIREMENT: 1, 11 (1.2, 1.3, 11.4)

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Implementing Cisco ASA firewalls in transparent mode helps reduce network complexity.
- IDS/IPS modules require the external network interface port to be connected to the network for management and automated reporting and alerts to be sent. For virtual modules, the Management 0 interface is used.
- When configuring high availability, only the primary Cisco ASA needs to be fully configured; the secondary Cisco ASA mirrors the primary's configurations once the failover interface and IP information are configured.

- Cisco Adaptive Security Device Manager (ADSM) is a good tool for making policy changes in small environments. For large enterprises, Cisco Security Manager provides the best platform for managing rules with a large number of objects across many devices.
- Multi-context firewalls allow for traffic and administrative segmentation.
- Firewall rule sets must adhere to a "least amount of access necessary" policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment (for example, point-of-sale) networks.
- Configure the primary login authentication of the Cisco ASA to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the Cisco ASA itself in the event of a WAN or Cisco Secure ACS failure.
- Configure logs to be sent to a centralized syslog server such as RSA enVision.
- Configure NTP to ensure all logging is coordinated
- Cisco ASA firewalls were used for the branch WAN, Internet edge, and data center aggregation block.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco ASA firewalls are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted.
- **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*
- **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

  The following configuration example shows how objects identify hosts and services within the network and their use in an access list to permit approved traffic:

```
!
! ----Naming of interfaces as assigned from the Admin Context----
!
interface outside
 nameif north
 bridge-group 1
 security-level 0
!
interface inside
```

```
 nameif south
 bridge-group 1
 security-level 100
!
! ----Defining Objects and Object Groups----
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 network-object 192.168.42.122 255.255.255.255
object-group network CSManager
 description Cisco Security Manager
 network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
 network-object 192.168.42.138 255.255.255.255
object-group network Admin-Systems
 group-object EMC-NCM
 group-object AdminStation
 group-object AdminStation2
 group-object CSManager
 group-object RSA-enVision
 group-object AdminStation3
 group-object AdminStation4-bart
!
object-group service CSM_INLINE_svc_rule_77309411635
 description Generated by CS-Manager from service of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ssh
 service-object tcp destination eq https
 group-object HTTPS-8443
!
object-group network CSM_INLINE_dst_rule_77309411635
 description Generated by CS-Manager from dst of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
 group-object DC-DMZ
!
! ----One line of the larger access-list permitting traffic----
!
access-list CSM_FW_ACL_south extended permit object-group
CSM_INLINE_svc_rule_77309411635 object-group Admin-Systems object-group
CSM_INLINE_dst_rule_77309411635
!
! ----Applying the access-list to an interface----
!
access-group CSM_FW_ACL_south in interface south
```

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

Cisco ASA firewalls allow only administrative connections from authorized hosts/networks, as specified in the device configuration. The HTTP server supports only secure connections using SSL. If no hosts or networks are specified for the service, it is effectively disabled (for example, the Telnet service). The following configuration shows the authorized management hosts for SSH and HTTPS administration, and none for Telnet.

```
http server enable
http 192.168.41.101 255.255.255.255 south
http 192.168.41.102 255.255.255.255 south
http 192.168.42.122 255.255.255.255 south
http 192.168.42.124 255.255.255.255 south
http 192.168.42.133 255.255.255.255 south
http 192.168.42.138 255.255.255.255 south
telnet timeout 5
ssh 192.168.41.101 255.255.255.255 south
ssh 192.168.41.102 255.255.255.255 south
ssh 192.168.42.122 255.255.255.255 south
ssh 192.168.42.124 255.255.255.255 south
ssh 192.168.42.133 255.255.255.255 south
ssh 192.168.42.138 255.255.255.255 south
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco ASA firewalls do not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco ASA firewalls support strong encryption for SSH and HTTPS. The following configurations are used to configure strong cryptography:

```
! ---Specify only Strong algorithms for SSL connections---
!
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1
!
! ---Specify strong encryption version of SSH
!
ssh version 2
!
```

  SNMP versions 1 and 2(c) transmit data between the SNMP server and the SNMP agent “in the clear”. This makes your infrastructure and corresponding infrastructure devices vulnerable to attack and or misuse. SNMP v3 adds authentication and privacy options to secure its communication between SNMP servers and SNMP agents.

  Cisco ASA firewalls allow secure administration using SNMP version 3 with encryption and authentication using the “priv” security model.

  SNMP groups provide an access control policy to which users are added. The user inherits the security model of the group.

  SNMP users are assigned a username, a group to which they belong, authentication password, encryption password, and associated algorithms to use. Authentication algorithms are MD5 and SHA. Encryption algorithms are DES, 3DES, and AES (128,192,256).

```
snmp-server enable
snmp-server group V3Group v3 priv
snmp-server user ciscolms V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
snmp-server user csmadmin V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
```

An SNMP host is the server to which SNMP notifications and traps are sent. SNMP v3 hosts require the SNMP server IP address and SNMP username. Each SNMP host can have only one username associated with it. The user credentials on the NMS (CiscoPrime, EMC NCM, and so on) must match the SNMP username credentials.

```
snmp-server host south 192.168.42.134 version 3 ciscolms
snmp-server host south 192.168.42.139 version 3 ciscolms
snmp-server host south 192.168.42.133 version 3 csmadmin

Enable the SNMP traps (this will change depending on environment and business
requirements). The following example enables all, but this could be limited to a
subset of traps.
snmp-server enable traps all
snmp-server location Building SJC-17-1 Aisle 1 Rack 3
snmp-server contact EmployeeA
```

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

Requirement 6: Develop and Maintain Secure Systems and Applications

PCI 6.1—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco ASA firewalls. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html.

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

To meet all of the requirements listed below, the PCI solution uses a centralized user database in the Active Directory, which is linked via LDAP, RADIUS, and TACACS+ services. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. This resource is used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco ASA firewalls are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco ASA firewalls, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (south) host 192.168.42.131
 key *****
aaa authentication ssh console RETAIL LOCAL
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
```

  Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

  These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication ssh console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco firewalls to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure Access Control Server must be implemented. Configure AAA services as shown above in requirement 7.

The firewall is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco firewalls support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
username csmadmin password <removed> encrypted privilege 15
```

```
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  When configuring local user accounts, you must specify a password to achieve PCI compliance. Do not use the "nopassword" option.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

- **PCI 8.3**—*Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.*

  Using AAA services, Cisco ASA firewalls can support two-factor authentication by pointing to an external authentication server (as described in Requirement 7). In the test environment, a second authentication service was set up using RSA Access Manager and SecurID tokens for generating one-time passwords. The following configurations show the setup of the additional AAA RADIUS server and authentication group for SSL VPN access from external sources.

```
aaa-server partnerauth protocol radius
aaa-server partnerauth (inside) host 192.168.42.137
 timeout 5
 key *****
 radius-common-pw *****

webvpn
 enable outside
 internal-password enable
 smart-tunnel list AllExternalApplications All-Applications * platform windows
group-policy DfltGrpPolicy attributes
 webvpn
  url-list value page1
  smart-tunnel enable AllExternalApplications
group-policy Retail-PCI internal
group-policy Retail-PCI attributes
 vpn-tunnel-protocol ssl-clientless
!
tunnel-group DefaultRAGroup general-attributes
 authentication-server-group partnerauth
tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group partnerauth
tunnel-group Retail-Lab type remote-access
tunnel-group Retail-Lab general-attributes
 authentication-server-group partnerauth LOCAL
 default-group-policy Retail-PCI
```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

All local passwords on the firewall are stored using strong encryption. Additionally, the following command can be used to encrypt local keys:

```
key config-key password-encryption
password encryption aes
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco ASA firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS or Cisco Security Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco ASA firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS or Cisco Security Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco ASA firewalls do not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco ASA firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco ASA firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco ASA firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco ASA firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco ASA firewalls are able to time-out administrative sessions using the following configuration statements:

```
!
http server idle-timeout 15
!
ssh timeout 15
!
console timeout 15
```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco ASA firewalls are able to track and monitor all administrative user access, events such as interface up/down, dropped or filtered traffic, device authentications, and VPN sessions, to name a few.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco ASA firewalls track individual administrator actions as identified in the requirements above (10.1, 10.2 and 10.3) through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging enable
logging timestamp
logging trap informational
logging asdm informational
logging host south 192.168.42.124
```

  Cisco ASA firewalls use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco ASA firewalls use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.162 source south
ntp server 192.168.62.161 source south prefer

clock timezone PST -8
clock summer-time PDT recurring
```

To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Note The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4**—*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco ASA Services Module (ASASM)—Data Center

The Cisco ASA Services Module (ASASM) is an integrated module installed inside a Cisco Catalyst 6500 Series Switch or Cisco 7600 Internet Router. The Cisco ASASM allows any port on the Cisco Catalyst switch to operate as a firewall port and integrates firewall security inside the network infrastructure.

The Cisco ASASM includes a number of advanced features that help reduce costs and operational complexity while enabling organizations to manage multiple firewalls from the same management platform. Features such as the resource manager help organizations limit the resources allocated to any security context at any time, thus ensuring that one security context does not interfere with another. The transparent firewall feature configures the Cisco ASASM to act as a Layer 2 bridging firewall, resulting in minimal changes to network topology.

Table 5-57 PCI Assessment Summary—Cisco ASA Services Module

Models Assessed
WS-SVC-ASA-SM1 version asa851-smp-k8.bin

Table 5-57 PCI Assessment Summary—Cisco ASA Services Module

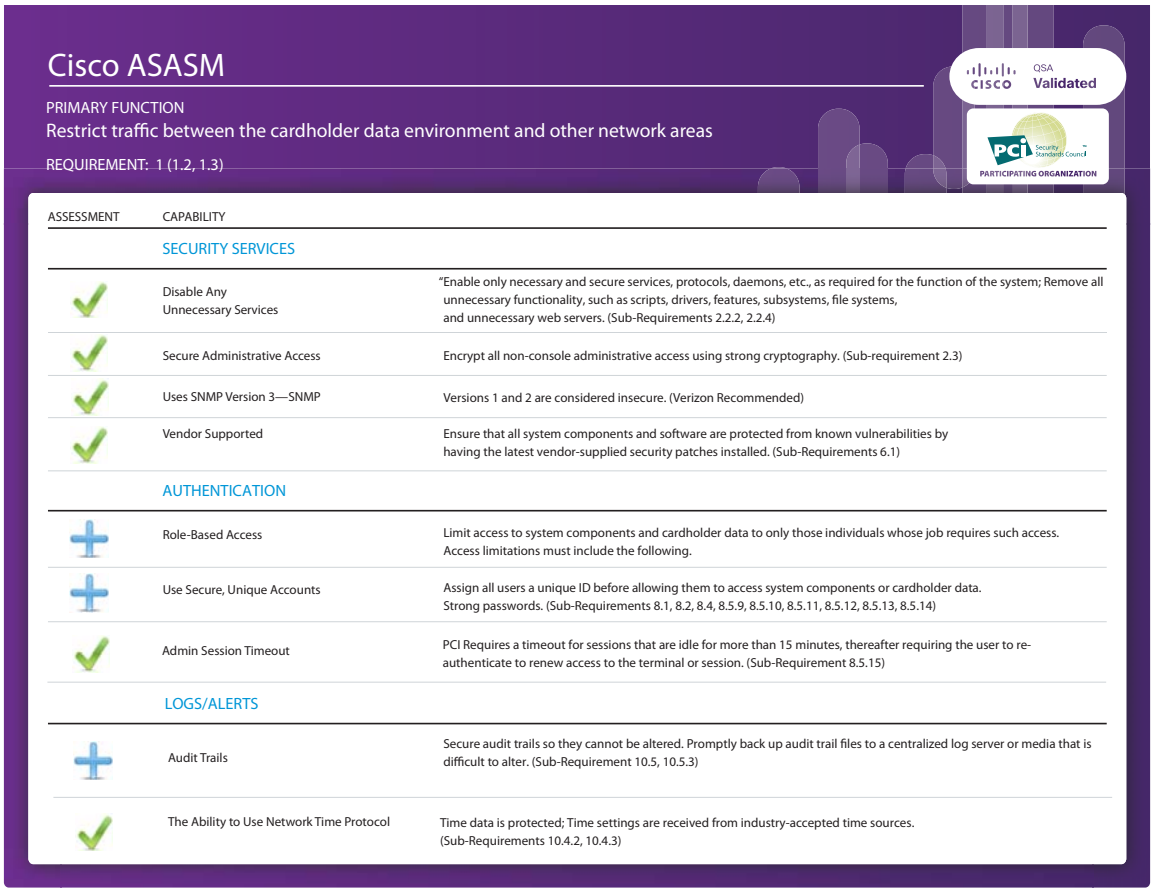
PCI Sub-Requirements Passed	
PCI 1	1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 4	4.1
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5..4
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function of the Cisco ASASM is to restrict traffic between the cardholder data environment and other areas of the network (1.2, 1.3).

Table 5-58 lists the component assessment details for the Cisco ASASM.

Table 5-58 Component Capability Assessment—Cisco ASA Services Module



Cisco ASASM

PRIMARY FUNCTION
Restrict traffic between the cardholder data environment and other network areas

REQUIREMENT: 1 (1.2, 1.3)

QSA Validated

PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
✓	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Firewall rule sets must adhere to a "least amount of access necessary" policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports.
- For Internet edge, disable **icmp permit** on the outside interface of Cisco ASASM. If users need to access servers in the DMZ segment, make sure that external users can reach the servers using very specific protocol and ports.
- Configure the **ip verify reverse path** command on all interfaces to provide anti-spoofing functionality.
- Configure the console timeout commands to 15 minutes or less on the console of the Cisco ASASM.
- Configure appropriate banner messages on login, incoming, and exec modes of the Cisco ASASM. The login banner warning should not reveal the identity of the company that owns or manages the Cisco ASASM. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the Cisco ASASM to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the Cisco ASASM itself in the event of connectivity or Cisco Secure ACS failure.
- Change default passwords and community strings to appropriate complexity.

- Allow only SSHv2 (and not Telnet or SSHv1) connection from network management station to Cisco ASASM.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco ASASM firewalls are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted.

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Firewall configuration files are backed up centrally using Cisco Prime LMS. These tools also verify that running and startup configurations of firewalls, routers, and switches are synchronized. Additionally, Cisco Security Manager stores a copy of the firewall configuration for the policies that it manages.

- **PCI 1.3**—*Prohibit direct public access between the Internet and any system component in the cardholder data environment.*

  Cisco ASASM firewalls track and monitor the state of communications and are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted. ASASM firewalls have multiple interfaces and VLAN support, allowing for segmentation of traffic and the creation of DMZ zones or areas with differing security policies. Cisco ASA firewalls can also perform NAT to aid in securing/obscuring the private IP addressing information used within an enterprise.

  - **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
  - **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
  - **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
  - **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
  - **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
  - **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
  - **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*
  - **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

  The following configuration example shows how objects identify hosts and services within the network and their use in an access list to permit approved traffic:

```
!
! ----VLAN's assigned from the Host Catalyst Switch----
!
interface Vlan21
 nameif inside
 security-level 100
 ip address 192.168.21.10 255.255.255.0
```

```
!
interface Vlan22
 nameif outside
 security-level 0
 ip address 192.168.22.1 255.255.255.0 standby 192.168.22.2
!!
! ----Defining Objects and Object Groups----
!
object-group network DC-ALL
 description All of the Data Center
 network-object 192.168.0.0 255.255.0.0
object-group network Stores-ALL
 description all store networks
 network-object 10.10.0.0 255.255.0.0
!
object-group service CSM_INLINE_svc_rule_81604379580 tcp
 description Generated by CS-Manager from service of FirewallRule# 7
(ASASM-DMZ-1_v1/mandatory)
 port-object eq smtp
 port-object eq https
 port-object eq ssh
!
object-group network CSM_INLINE_src_rule_81604379580
 description Generated by CS-Manager from src of FirewallRule# 7
(ASASM-DMZ-1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
! ----One line of the larger access-list permitting traffic----
!
access-list INSIDE extended permit tcp object-group CSM_INLINE_src_rule_81604379580
192.168.23.64 255.255.255.224 object-group CSM_INLINE_svc_rule_81604379580
!
! ----Applying the access-list to an interface----
!
access-group INSIDE in interface inside
```

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco ASASM firewalls allow only administrative connections from authorized hosts/networks, as specified in the device configuration. The HTTP server supports only secure connections using SSL. If no hosts or networks are specified for the service, it is effectively disabled (for example, the Telnet service). The following configuration shows the authorized management hosts for SSH and HTTPS administration, and none for Telnet.

```
http server enable
http 192.168.41.101 255.255.255.255 inside
http 192.168.41.102 255.255.255.255 inside
http 192.168.42.122 255.255.255.255 inside
http 192.168.42.124 255.255.255.255 inside
http 192.168.42.133 255.255.255.255 inside
http 192.168.42.138 255.255.255.255 inside

ssh 192.168.41.101 255.255.255.255 inside
ssh 192.168.41.102 255.255.255.255 inside
ssh 192.168.42.122 255.255.255.255 inside
ssh 192.168.42.124 255.255.255.255 inside
ssh 192.168.42.133 255.255.255.255 inside
```

```
ssh 192.168.42.138 255.255.255.255 inside
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco ASASM firewalls do not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco ASASM firewalls support strong encryption for SSH and HTTPS. The following configurations are used to configure strong cryptography:

```
! ---Specify only Strong algorithms for SSL connections---
!
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1
!
! ---Specify strong encryption version of SSH
!
ssh version 2
!
```

SNMP versions 1 and 2(c) transmit data between the SNMP server and the SNMP agent “in the clear”. This makes your infrastructure and corresponding infrastructure devices vulnerable to attack and or misuse. SNMP v3 adds authentication and privacy options to secure its communication between SNMP servers and SNMP agents.

Cisco ASA firewalls allow secure administration using SNMP version 3 with encryption and authentication using the “priv” security model.

SNMP groups provide an access control policy to which users are added. The user inherits the security model of the group.

SNMP users are assigned a username, a group to which they belong, authentication password, encryption password, and associated algorithms to use. Authentication algorithms are MD5 and SHA. Encryption algorithms are DES, 3DES, and AES (128,192,256).

```
snmp-server enable
snmp-server group V3Group v3 priv
snmp-server user ciscolms V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
snmp-server user csmadmin V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
```

An SNMP host is the server to which SNMP notifications and traps are sent. SNMP v3 hosts require the SNMP server IP address and SNMP username. Each SNMP host can have only one username associated with it. The user credentials on the NMS (CiscoPrime, EMC NCM, and so on) must match the SNMP username credentials.

```
snmp-server host south 192.168.42.134 version 3 ciscolms
snmp-server host south 192.168.42.139 version 3 ciscolms
snmp-server host south 192.168.42.133 version 3 csmadmin
```

Enable the SNMP traps (this will change depending on environment and business requirements). The following example enables all, but this could be limited to a subset of traps.

```
snmp-server enable traps all
snmp-server location Building SJC-17-1 Aisle 1 Rack 3
snmp-server contact EmployeeA
```

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco ASASM modules. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

  For more information about PSIRT:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco ASASM firewalls are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco ASASM firewalls, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (south) host 192.168.42.131
 key <removed>
aaa authentication ssh console RETAIL LOCAL
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
```

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication ssh console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco firewalls to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure Access Control Server must be implemented. Configure AAA services as shown above in requirement 7.

The firewall is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco firewalls support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username csmadmin password <removed> encrypted privilege 15
  username retail password <removed> encrypted privilege 15
  username bmcgloth password <removed> encrypted privilege 15
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  When configuring local user accounts, you must specify a password to achieve PCI compliance.

  Do NOT use the “nopassword” option.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  All local passwords on the firewall are stored using strong encryption. Additionally, the following command can be used to encrypt local keys:

  ```
  password encryption aes
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco ASASM firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS or Cisco Security Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco ASASM firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Prime LMS or Cisco Security Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco ASASM firewalls do not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco ASASM firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco ASASM firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco ASASM firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco ASASM firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco ASASM firewalls are able to time-out administrative sessions using the following configuration statements:

  ```
  !
  http server idle-timeout 15
  ```

```
!
ssh timeout 15
!
console timeout 15
```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco ASASM firewalls are able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco ASASM firewalls use the local clock facilities of the host Cisco Catalyst chassis to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

  The Cisco ASASM uses the clock of the Cisco Catalyst chassis as configured in the Supervisor Module.

To meet all of the requirements listed below, the PCI solution uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*

- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Virtual Security Gateway

The Cisco Virtual Security Gateway (VSG) for Cisco Nexus 1000V Series Switches was used in the data center for setting a boundary between the sensitive scope of the organization's cardholder data environment and out-of-scope networks. It is a virtual firewall for Cisco Nexus 1000V Series Switches that delivers security and compliance for virtual computing environments. Cisco VSG uses virtual service data path (vPath) technology embedded in the Cisco Nexus 1000V Series Virtual Ethernet Module (VEM), offering transparent firewall insertion and efficient deployment. All the policy management for VSG is done via Virtual Network Management Center (VNMC). Cisco VSG provides the following:

- Zone-based security controls based on network as well as virtual machine attributes. This flexibility simplifies security policies, which are easy to troubleshoot and audit.
- Secure multi-tenant deployment, protecting tenant workloads on a shared compute infrastructure.
- Leverages vPath intelligence for efficient network-wide deployment and accelerated performance through fast-path off-load.
- IT security, network, and server teams to collaborate while helping ensure administrative segregation to meet regulatory and audit requirements and reduce administrative errors.

Primary PCI Function

The main function of the Cisco VSG is segmentation of PCI scope and enforcement of that new scope boundary. The Cisco VSG serves as a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network. (1.2, 1.3)

Table 5-59 PCI Assessment Summary—Cisco VSG

Models Assessed	
Nexus VSG version 4.2(1)VSG1(1)	
PCI Sub-Requirements Passed	
PCI 1	1.2.1, 1.2.2, 1.3.5, 1.3.6, 1.3.7
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5

Table 5-59 PCI Assessment Summary—Cisco VSG

PCI Sub-Requirements Requiring Compensating Controls
No compensating controls were required to satisfy any sub-requirements.
PCI Sub-Requirements Failed
No sub-requirements were failed.

Table 5-60 lists the component assessment details for the Cisco VSG.

Table 5-60 Component Capability Assessment—Cisco VSG



Cisco VSG

PRIMARY FUNCTION
Restrict traffic between the cardholder data environment and other network areas

REQUIREMENT: 1 (1.2, 1.3)

cisco QSA Validated

PCI Security Standards Council PARTICIPATING ORGANIZATION

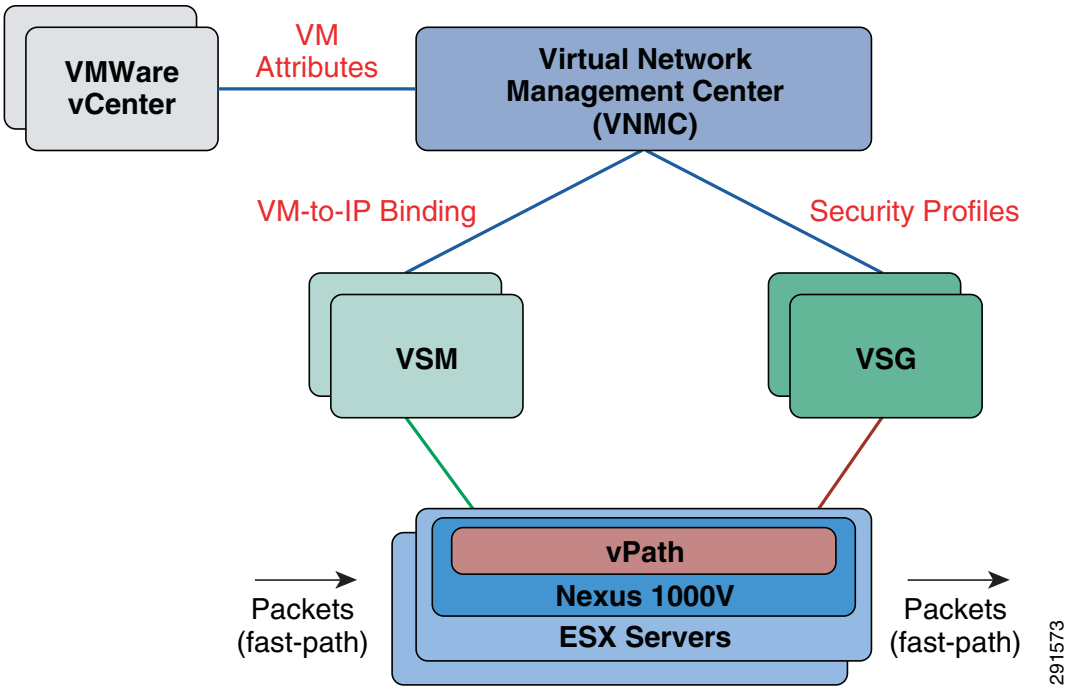
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
✓	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

Cisco VSG integrates with Cisco Nexus 1000V Series Switches to enforce security policies for your virtualized environment. VNMC provides policy management for a multitenant environment. One or more VSGs are required per tenant. VSG uses the vPath intelligence in the Virtual Ethernet Module (VEM) of the Cisco Nexus 1000V Series to provide the security policy enforcement.

Cisco VSG is deployed as a virtual appliance in vCenter. The primary function of Cisco VSG is to protect against unauthorized access to the cardholder environment.

Figure 5-132 Cisco Nexus VSG System Architecture



PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

Cisco VSG can protect the cardholder data environment from untrusted networks by enforcing security policies for any network traffic entering or leaving a virtual machine. These security policies are enabled at a port-profile level in the Cisco Nexus 1000V. All the virtual machines connecting to the network with those port-profiles (port-groups) are protected through firewall policies.

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*
- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Configuration files are backed up centrally using Cisco Prime LMS. This tool also verifies that running and startup configurations of devices are synchronized.
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*

To insert the firewall into the network, you need to attach the security profile to the port profile. All the traffic traversing through the virtual ports associated with that port profile, is enforced by the security policy. The following two commands enable the firewall feature under the port profile:

```
Nexus1000V (config)# org root/TenantA
Nexus1000V (config)# vn-service ip-address VSG_Data_IP vlan VSG_Service_VLAN
security-profile SecureTenantA
```

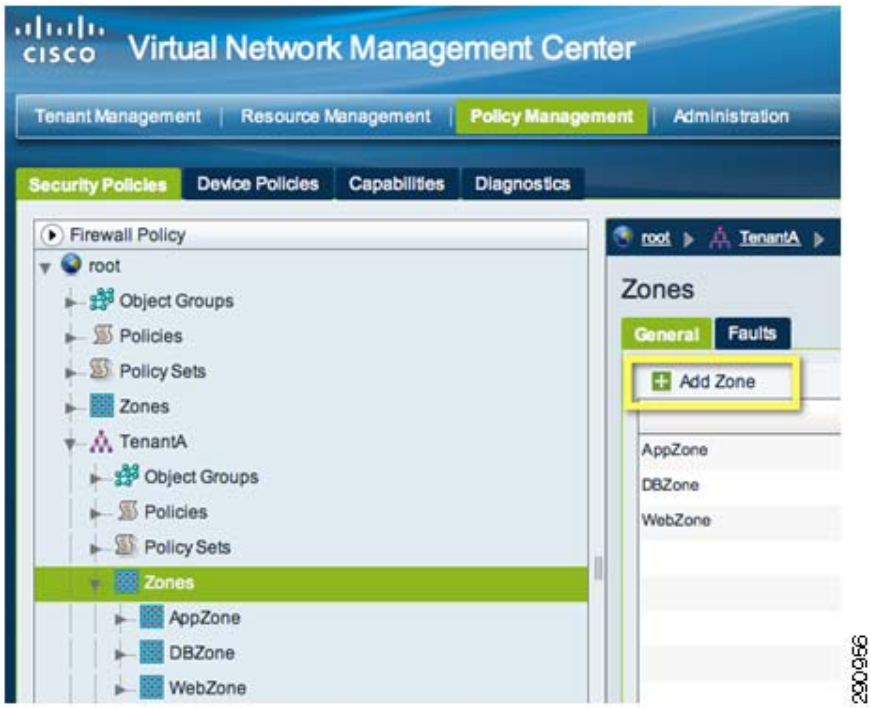
The first command specifies the tenant whose workload is being protected. The second command binds the security profile to the port-profile for that tenant. Once the firewall is enabled, the traffic is intercepted by vPath and sent to Cisco VSG over a dedicated VLAN. Cisco VSG evaluates the traffic against the security policy. It sends the decision (deny or allow) back to vPath, which enforces the Cisco VSG decision to the traffic flow. VNMC publishes the security policies for each tenant for individual Cisco VSGs. These policies are maintained and edited in the VNMC.

Placing cardholder data systems in security zones can isolate the environment from the DMZ and external network. These zones are leveraged in writing the security policies in the VNMC.

To create the Navigation pane, do the following:

1. Click the Policy Management tab, click the Security Policies subtab, and expand Firewall Policy > root to view the appropriate Zones node.
2. Select the organizational level (Tenant) where you want to add the zone. In the Work pane, click the Add Zone link. (See Figure 5-133.)

Figure 5-133 Virtual Network Management Center—Policy Management



Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Nexus VSG does not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Only SSH access is allowed for firewall console access over the network. The communication between Cisco VSG and Management Platform (VNMC) is all encrypted over SSL (443)

  Cisco Nexus VSG can be configured to use secure protocols for all system functions. This includes SSH for remote management, SCP, and SFTP for file transfers. Insecure services can be disable or blocked using configuration statements and access lists.

  ```
  no feature telnet
  no telnet server enable
  feature ssh
  ```

  Cisco Nexus VSG support administrative protocols with strong cryptography such as SSH version 2.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Nexus Virtual Security Gateway. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html.

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

  For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by the Cisco Nexus VSG using LDAP services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  User roles in VNMC contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has policy-related privileges, and Role2 has tenant-related privileges, users who are assigned to both Role1 and Role2 have policy and tenant related privileges.

  The system contains the following default user roles:

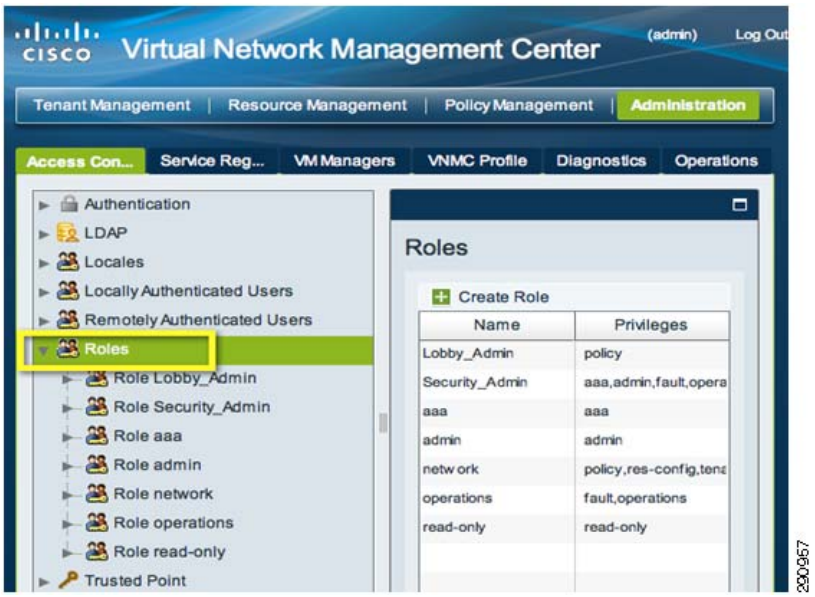
  - aaa—User has read and write access to users, roles, and AAA configuration. Read access to the rest of the system.
  - admin—User has complete read-and-write access to the entire system and has all privileges. The default admin account is assigned this role by default, and it cannot be changed.
  - network—User creates organizations, security policies, and device profiles.
  - operations—User acknowledges faults and performs some basic operations such as logging configuration.
  - read-only—User has read-only access to system configuration and operational status with no privileges to perform any operations.

  Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Network and Operations roles have different sets of privileges, but a new Network and Operations role can be created that combines the privileges of both roles.

  To configure roles in VNMC, do the following:

  1. Click the **Administration** tab, then click the **Access Control** sub-tab.
  2. In the Navigation pane, select the **Roles** node. In the Work pane, click **Create Roles** (see Figure 5-134.)

Figure 5-134 Configuring Roles



In addition to roles, the user is also provided another dimension of privilege, which limits the user to tenant level visibility, called *locale*. Each locale defines one or more organizations (domains) to which the user is allowed access, and access would be limited to the organizations specified in the locale. To configure locales in VNMC, do the following:

1. Click the Administration tab, then click the Access Control sub-tab.
2. In the Navigation pane, select the Locales node.
3. In the Work pane, click the Create Locale link. (See Figure 5-135.)

Figure 5-135 Configuring Locales



CLI configuration of AAA services is as follows:

```
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
!
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the LDAP authentication capabilities to the Windows Active Directory server for AAA services. Microsoft Active Directory contains the necessary user account services for all of the appropriate PCI 8 requirements. Configure AAA services as shown above in Requirement 7.

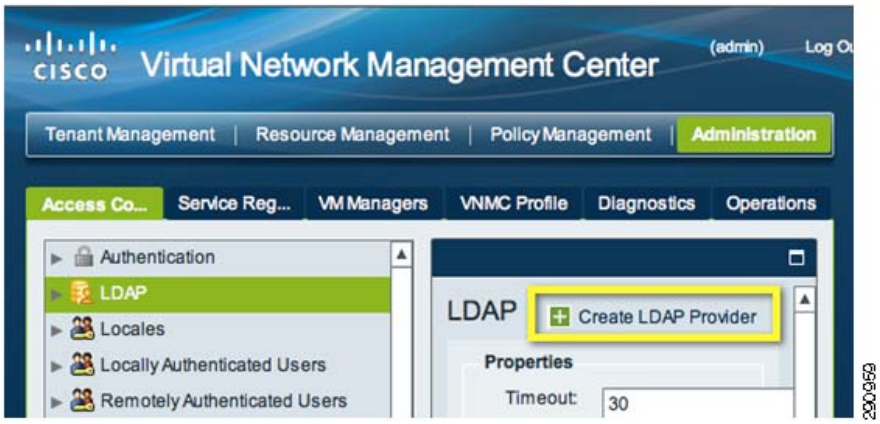
- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco VNMC provides remote authentication with LDAP servers for user authentication. When user accounts are created in the LDAP server, the accounts also include the roles and locales those users require for working in Cisco VNMC.

  To configure the LDAP server, do the following:

  1. Click the Administration tab, the click the Access Control sub-tab.
  2. In the Navigation pane, select the LDAP node.
  3. In the Work pane, click the Create LDAP Provider link. (See Figure 5-136.)

Figure 5-136 Configuring LDAP Server



Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco Nexus VSG is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Nexus VSG uses NTP to update and synchronize local clock facilities and meet the following requirements:

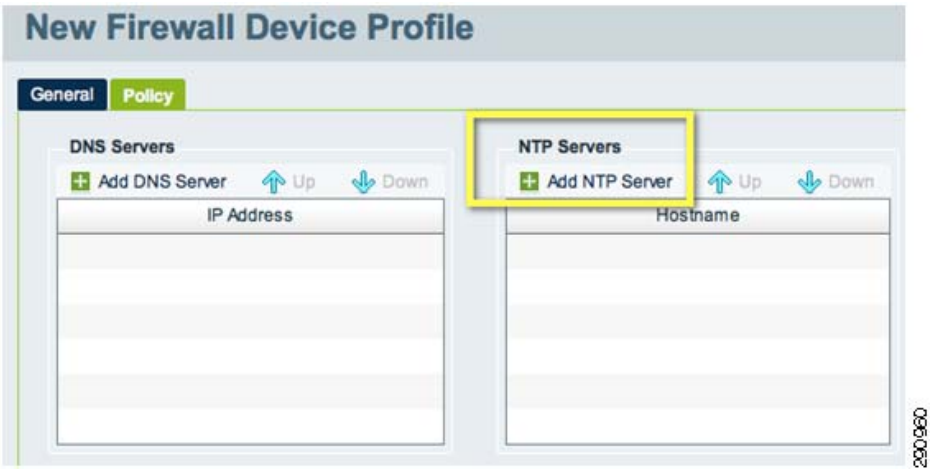
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

NTP is configured in the Firewall Device Profile for the Cisco VSG VNMC. The setting is published via the device policy to Cisco VSG.

1. In the navigation pane, click the Policy Management tab, then the Device Policies sub-tab, and expand the Device Profile for a tenant.
2. Click a Profiles node to add a firewall device profile, and you see the option to add NTP server, as shown in Figure 5-137.

Figure 5-137 Configuring NTP



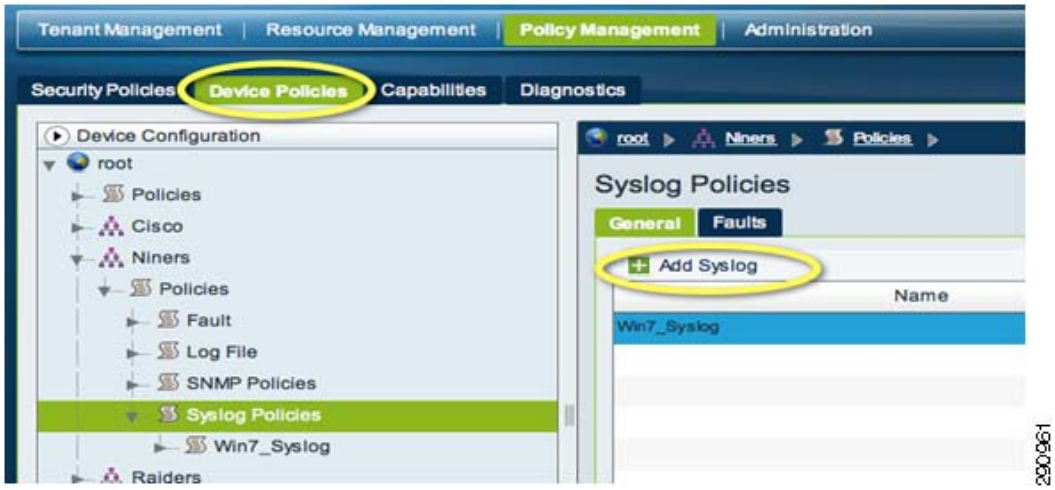
Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  You can configure the syslog server for Cisco VSG to send all the logging information to a standard syslog server. This setting is available as part of the device profile.

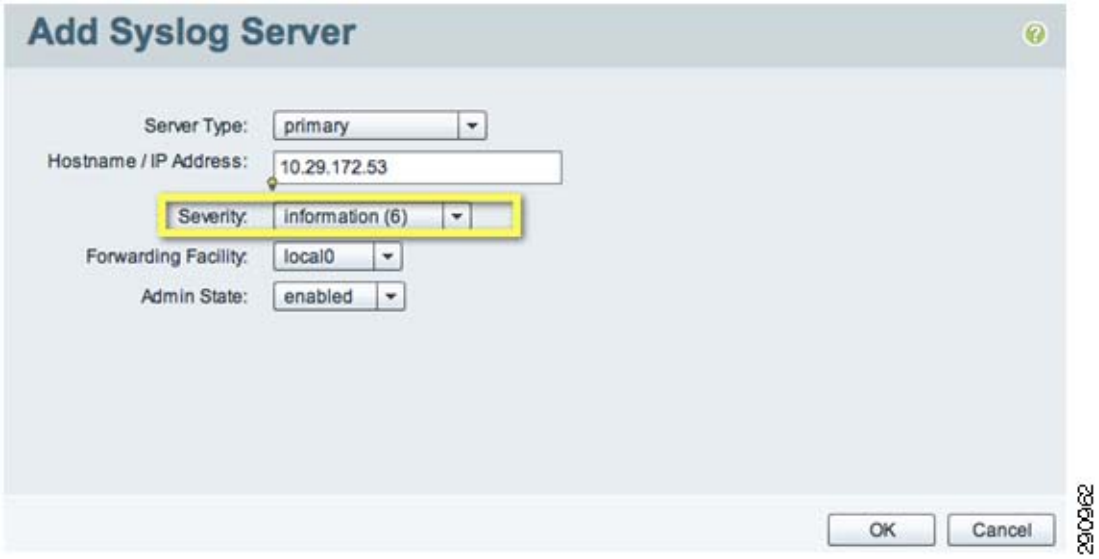
  1. Navigate to Policy Management > Device Policies > Tenant> Policies > Syslog Policies. Add a syslog policy, as shown in Figure 5-138.

Figure 5-138 Configuring Syslog



2. The severity of the logging should be at level 6 to capture the firewall policy hit in the VSG. (See Figure 5-139).

Figure 5-139 Configuring Logging Severity



3. The syslog policy is attached to the Device Profile to enable the settings in the VSG.

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Intrusion Detection

Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2

The Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM2) is an important intrusion prevention system (IPS) solution that protects switched environments by integrating full-featured IPS functions directly into the network infrastructure through the widely deployed Cisco Catalyst chassis. This integration allows the user to monitor traffic directly off the switch backplane.

The Cisco IDSM-2 with Cisco IPS Sensor Software v6.0 helps users stop more threats with greater confidence, through the use of the following elements:

- Multivector threat identification—Detailed inspection of Layer 2–7 traffic protects your network from policy violations, vulnerability exploitations, and anomalous activity.
- Accurate prevention technologies—The innovative Cisco Risk Rating feature and Meta Event Generator provide the confidence to take preventive actions on a broader range of threats without the risk of dropping legitimate traffic.

When combined, these elements provide a comprehensive inline prevention solution, providing the confidence to detect and stop the broadest range of malicious traffic before it affects business continuity.

Table 5-61 PCI Assessment Summary—Cisco IDSM2

Models Assessed	
WS-SVC-IDSM-2 version 7.0(4)	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.4
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary PCI function of the Cisco ISDM2 is to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises (11.4).

Table 5-62 lists the component assessment details for the Cisco ISDM2.

Table 5-62 Component Capability Assessment—Cisco ISDM2



Cisco ISDM

PRIMARY FUNCTION
Monitor all traffic at the perimeter of the CDE as well as all critical points inside the CDE

REQUIREMENT: 11 (11.4)

QSA Validated

PARTICIPATING ORGANIZATION

ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
✓	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
✓	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
✓	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
+	Role-Based Access	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following.
+	Use Secure, Unique Accounts	Assign all users a unique ID before allowing them to access system components or cardholder data. Strong passwords. (Sub-Requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re-authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	Audit Trails	Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Sub-Requirement 10.5, 10.5.3)
✓	The Ability to Use Network Time Protocol	Time data is protected; Time settings are received from industry-accepted time sources. (Sub-Requirements 10.4.2, 10.4.3)

Design Considerations

- Configure the Cisco IDSM2 to lock accounts so that users cannot keep trying to login after a certain number of failed attempts.
- Allow secure management of the Cisco IDSM2 only from a specific host/hosts.
- Configure appropriate banner messages on login. The login banner warning should not reveal the identity of the company that owns or manages the Cisco IDSM2. The banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Change default passwords and community strings to appropriate complexity.

For more information, see the Installation Guide at the following URL:
http://www.cisco.com/en/US/docs/security/ips/6.0/configuration/guide/cli/cliInter.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

Cisco IDSM2 modules allow only administrative connections from authorized hosts/networks as specified in the device configuration. The following configuration shows the authorized management hosts for SSH and HTTPS administration, and disabling of Telnet.

```
! ------------------------------
service host
network-settings
host-ip 192.168.21.94/24,192.168.21.1
host-name DMZ-IDS2
telnet-option disabled
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.138/32
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco IDSM2 modules do not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco IDSM2 modules use strong encryption for SSH and HTTPS.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco IDSM2 modules. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

  The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

  For more information about PSIRT:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS RADIUS services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco IDSM2 modules are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements use the RADIUS protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
! ------------------------------
service aaa
aaa radius
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id DMZ-IDS1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! ------------------------------
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services, as shown above in Requirement 7.

The Cisco IDSM2 module is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco IDSM2 modules support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  sensor(config)# username username password password privilege
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something yo*u are, such as a biometric

  When configuring local user accounts, you must specify a password to achieve PCI compliance.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  All local passwords on the Cisco IDSM2 are stored using strong encryption.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco IDSM2 modules do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco IDSM2 modules do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco IDSM2 modules support the ability to specify a minimum password length for local accounts.

```
! ------------------------------
service authentication
password-strength
size 7-64
! ------------------------------
```

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco IDSM2 modules support the ability to specify alphanumeric passwords for local accounts.

```
! ------------------------------
service authentication
password-strength
digits-min 1
lowercase-min 1
other-min 1
! ------------------------------
```

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco IDSM2 modules support the ability to specify that old passwords should not be re-used for local accounts.

```
! ------------------------------
service authentication
password-strength
number-old-passwords 4
! ------------------------------
```

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco IDSM2 modules support the ability to specify that only a limited number of attempts can be made when authenticating for local accounts.

```
! ------------------------------
service authentication
attemptLimit 6
! ------------------------------
```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

Cisco IDSM2 modules support the ability to lockout local accounts after the specified number of failed attempts, requiring an administrator to re-enable them. Locked accounts are indicated by parentheses when using the **show users** command:

```
sensor# show users all
    CLI ID   User         Privilege
*   1349     bart         administrator
    5824     (pauljones)  viewer
    9802     christian    operator
```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco IDSM2 modules do not feature an explicit session timeout. Administration time limits would need to be enabled systemically through active directory policy to the admin workstation desktops.



Note IPS Software version 7.1.x and newer supports a CLI activity timer addressing this desired functionality. To enable, enter the "cli-inactivity-timeout 15" command in the Service Authentication portion of the configuration.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco IDSM2 is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco IDSM2 uses NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco IDSM2 uses NTP to meet these requirements by implementing the following configuration statements:

```
time-zone-settings
offset -8
standard-time-zone-name PST
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 192.168.62.161
exit
summertime-option recurring
summertime-zone-name PDT
```

To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Note The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution uses a central logging repository located in the data center. RSA enVision collects information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco IDSM2 modules are capable of sending system events to a centralized repository using SNMP traps. Logs stored locally are buffered and require operator level privileges on the device to be viewed. External logging is enabled by implementing the following configuration statements to send them to the RSA enVision server:

```
! ------------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name RSAenVision
exit
enable-notifications true
trap-community-name RSAenVision
exit
! ------------------------------
```

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4**—*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.*

  Cisco IDSM2 modules are capable of performing intrusion detection and prevention through the use of VLAN interfaces from the host Cisco Catalyst service chassis. IPS signature updates and configurations are managed centrally through Cisco Security Manager. The following configuration statements are necessary in the Cisco Catalyst service chassis to forward traffic via VLANs and enable the IDS inspection capability:

```
!
!
intrusion-detection module 2 management-port access-vlan 21
intrusion-detection module 2 data-port 1 trunk allowed-vlan 83,84
!
```

  Cisco IDSM2 module interfaces are configured as follows to receive, inspect, and forward traffic across the assigned VLANs:

```
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/7
subinterface-type inline-vlan-pair
subinterface 1
description INT1 vlans 83 and 84
vlan1 83
vlan2 84
exit
exit
exit
exit
! ------------------------------
```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.



CHAPTER 6

Summary

PCI can be simplified. Moreover, enterprise-class business can be simplified. The Cisco enterprise architecture provides the core infrastructure and principles for minimizing the complexity of running large-scale organizations. When combined with Cisco's strategic partners, compliance challenges are met with a comprehensive and unique approach that stands alone in the industry.

Compliance is a journey, not a destination. It requires continual attention to maintain. It is a journey that cannot be traveled alone. Trusted advisors such as auditors and vendors simplify the goal of maintaining compliance. The following provides a summary of the PCI assessment results.

Cisco Compliance Solution Components

This solution combines components to create an end-to-end solution conforming to the requirements of the PCI 2.0 guidelines. The result is a set of branch, data center, and Internet edge architectures and designs that simplify the process of achieving and maintaining compliance.

Endpoints	Primary PCI Function
Cisco IronPort Email Security	DLP
Cisco Physical Access Control	9.1
Cisco UCS and UCS Express	Servers
Cisco Unified CM and IP Phones	9.1.2
Cisco Video Surveillance	9.1.1
Administration	**Primary PCI Function**
Cisco ACS	7.1
Cisco Identity Services Engine	7.1, 11.1b, 11.1d
Cisco Prime LMS	1.2.2
Cisco Security Manager	1.2
Hytrust Appliance	10.5
RSA Authentication Manager	8.3
RSA Data Protection Manager	3.5
RSA enVision	10.5

Infrastructure	Primary PCI Function
Cisco ASA-Branch	1.3, 11.4
Cisco ASA-Data Center	1.3, 11.4
Cisco Branch Routers	1.3, 11.4
Cisco Branch Switches	Segmentation
Cisco Data Center Routers	1.2, 1.3
Cisco Data Center Switches	Segmentation
Cisco Data Center IDSM	11.4
Cisco MDS Switches	3.4
Cisco Nexus 1000V Series Switch	Segmentation
Cisco Nexus Data Center Switches	Segmentation
Cisco Nexus VSG	Virtual Firewall
Cisco Wireless	4.1, 11.1
EMC CLARiioN SAN	Storage



APPENDIX A

Bill Of Material

Branch—MSP Branch

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	5
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	Cisco 1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	5
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	5
CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	Cisco SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	5
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	5
AIR-WLC2125-K9	AIR-WLC2125-K9	Cisco	Cisco 2100 Series WLAN Controller for up to 25 Lightweight APs	1
ASA5505-PWR-AC	ASA5505-PWR-AC	Cisco	Cisco ASA 5505 AC Power Supply Adapter	1
SSC-BLANK	SSC-BLANK	Cisco	Cisco ASA 5505 SSC Blank Slot Cover	1
SWLC2100K9-70-ER	SWLC2100K9-70-ER	Cisco	Cisco Unified Wireless Controller SW Release 7.0	1
CAB-AC-C5	CAB-AC-C5	Cisco	AC Power Cord, Type C5, US	1
CON-SNT-AC2125K9	CON-SNT-AC2125K9	Cisco	SMARTNET 8X5XNBD WLAN Controller	1
SWLC2100K9-70	SWLC2100K9-70	Cisco	Cisco Unified Wireless Controller SW Release 7.0	1

ASA5515-IPS-K9	ASA5515-IPS-K9	Cisco	ASA 5515-X with IPS, SW, 6GE Data, 1GE Mgmt, AC, 3DES/AES	1
ASA5500-SC-5	ASA5500-SC-5	Cisco	ASA 5500 5 Security Contexts License	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
SF-ASA-9.1-K8	SF-ASA-9.1-K8	Cisco	ASA 5500 Series Software Ver. 9.1 for ASA 5512X--5555X, DES	1
SF-ASAIPS64-7.1-K9	SF-ASAIPS64-7.1-K9	Cisco	ASA 5500-X IPS Software 7.1 for IPS SSP	1
ASA5515-IPS-SSP	ASA5515-IPS-SSP	Cisco	ASA 5515-X IPS SSP License	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
CON-OSP-ASAUC24	CON-OSP-ASAUC24	Cisco	ONSITE 24X7X4 ASA-UC-24	1
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	1
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	1
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1

CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	1
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	1
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	1
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	1
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	1
CIVS-MSP-1RU	CIVS-MSP-1RU	Cisco	1RU MSP Assembly	1
CIVS-CAB-16-AC	CIVS-CAB-16-AC	Cisco	CIVS C16 Power Cable North America	1
CIVS-HDD-1000	CIVS-HDD-1000	Cisco	1TB SATA Drive for CIVS-MSP	4
CIVS-MS-SW6.2	CIVS-MS-SW6.2	Cisco	CIVS-MS Media Server v6.2 Software License with Hardware	1
CIVS-VSM-SW4262	CIVS-VSM-SW4262	Cisco	CIVS-VSM Video Surveillance Manager v4.2/6.2 SW Mfg Image	1
CON-SNT-VSM1U	CON-SNT-VSM1U	Cisco	SMARTNET 8X5XNBD 1RU MSP Assembly	1
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	1
CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	1
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C2960S-48FPS-L	WS-C2960S-48FPS-L	Cisco	Catalyst 2960S 48 GigE PoE 740W, 4 x SFP LAN Base	1
CAB-L620P-C13-US	CAB-L620P-C13-US	Cisco	Power Cord, 250VAC, 15A, NEMA L6-20 to C13, US	1

Branch—Convenience Branch

Name	Catalog Num	Vendor	Description	Qty
AIR-LAP1042N-A-K9	AIR-LAP1042N-A-K9	Cisco	802.11a/g/n Fixed Unified AP; Int Ant; A Reg Domain	1
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	1
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	1
CON-SNT-L1042A	CON-SNT-L1042A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Fixed Un	1
S104RK9W-12423JA	S104RK9W-12423JA	Cisco	Cisco 1040 Series IOS WIRELESS LAN LWAPP RECOVERY	1
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	1
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	1
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	1
CISCO891W-AGN-A-K9	CISCO891W-AGN-A-K9	Cisco	Cisco 891 GigaE SecRouter w/ 802.11n a/b/g FCC Comp	1
AIR-ANTM2050D-R	AIR-ANTM2050D-R	Cisco	2.2dBi/2.4Ghz,5.0dBi/5GHz DualBand Dipole Antenna	3
CAB-AC2	CAB-AC2	Cisco	AC Power cord North America	1
CAB-ETH-S-RJ45	CAB-ETH-S-RJ45	Cisco	Yellow Cable for Ethernet, Straight-through, RJ-45, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-80W-AC	PWR-80W-AC	Cisco	Power Supply 80 Watt AC	1
S890VK9-15001M	S890VK9-15001M	Cisco	Cisco 890 Series IOS UNIVERSAL	1
SL-890-AIS	SL-890-AIS	Cisco	Cisco 890 Advanced IP Services License	1
800-IL-PM-4	800-IL-PM-4	Cisco	4 Port 802.3af capable pwr module for 890 Series Router	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-C891WAK9	CON-SNT-C891WAK9	Cisco	SMARTNET 8X5XNBD Cisco 891 GigaE SecRouter	1
MEM8XX-512U768D	MEM8XX-512U768D	Cisco	DRAM Upgrade 512 MB to 768 MB	1

CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
WS-C2960PD-8TT-L	WS-C2960PD-8TT-L	Cisco	Catalyst 2960 Powered Device 8 10/100 + 1 1000BT LAN Base	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-C2960P8T	CON-SNT-C2960P8T	Cisco	SMARTNET 8X5XNBD Cat2960 Pwrd Device 8 10/100-1 1K BT LAN	1
PWR-A	PWR-A	Cisco	Pwr Sply In:100-240VAC Out:48VDC 380mA-2960PD-8TT-L	1

Branches—Mini Branch

Name	Catalog Num	Vendor	Description	Qty
AIR-LAP1042N-A-K9	AIR-LAP1042N-A-K9	Cisco	802.11a/g/n Fixed Unified AP; Int Ant; A Reg Domain	1
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	1
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	1
CON-SNT-L1042A	CON-SNT-L1042A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Fixed Un	1
S104RK9W-12423JA	S104RK9W-12423JA	Cisco	Cisco 1040 Series IOS WIRELESS LAN LWAPP RECOVERY	1
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	1
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	1
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	1

CISCO1941W-A/K9	CISCO1941W-A/K9	Cisco	Cisco 1941 Router w/ 802.11 a/b/g/n FCC Compliant WLAN ISM	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
S801RK9W-12421JA	S801RK9W-12421JA	Cisco	Cisco 801 Series IOS WIRELESS LAN LWAPP RECOVERY	1
S801W7K9-12421JA	S801W7K9-12421JA	Cisco	Cisco 801 Series IOS WIRELESS LAN	1
SL-19-IPB-K9	SL-19-IPB-K9	Cisco	IP Base License for Cisco 1900	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-1941WA	CON-SNT-1941WA	Cisco	SMARTNET 8X5XNBD Cisco 1941 Router w/ 802.11 a/b/g/n FCC	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
MEM-1900-512U2.5GB	MEM-1900-512U2.5GB	Cisco	512MB to 2.5GB DRAM Upgrade (2GB+512MB) for Cisco 1941 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
PWR-1941-POE	PWR-1941-POE	Cisco	Cisco 1941 AC Power Supply with Power Over Ethernet	1
S19UK9-15102T	S19UK9-15102T	Cisco	Cisco 1900 IOS UNIVERSAL	1
SL-19-SEC-K9	SL-19-SEC-K9	Cisco	Security License for Cisco 1900	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
WS-C2960G-8TC-L	WS-C2960G-8TC-L	Cisco	Cisco Catalyst 2960 7 10/100/1000 + 1 T/SFP LAN Base	2

CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	2
CON-SNT-C2960G8C	CON-SNT-C2960G8C	Cisco	SMARTNET 8X5XNBD Catalyst 2960 7 10/1	2
GLC-SX-MM=	GLC-SX-MM=	Cisco	GE SFP, LC connector SX transceiver	2
PWR-CLIP	PWR-CLIP	Cisco	Power retainer clip for compact switches	2
RCKMNT-19-CMPCT=	RCKMNT-19-CMPCT=	Cisco	19in RackMount for Cisco Catalyst 3560,2960,ME-3400 Compact Switch	2

Branches—Small Branch

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502E-A-K9	AIR-CAP3502E-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Ext Ant; A Reg Domain	2
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	2
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	2
AIR-ANT2422DW-R	AIR-ANT2422DW-R	Cisco	2.4 GHz 2.2 dBi Swivel Dipole Antenna White, RP-TNC	6
AIR-ANT5135DW-R	AIR-ANT5135DW-R	Cisco	5 GHz 3.5 dBi Swivel Dipole Antenna White, RP-TNC	6
CON-SNT-CAP3502A	CON-SNT-CAP3502A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; E	2
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	2
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	2
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	2
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	2
CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	2
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	2
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	2
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	2

CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	2
CISCO2921-SEC/K9	CISCO2921-SEC/K9	Cisco	Cisco 2921 Security Bundle w/SEC license PAK	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-2921-51-AC	PWR-2921-51-AC	Cisco	Cisco 2921/2951 AC Power Supply	1
SL-29-IPB-K9	SL-29-IPB-K9	Cisco	IP Base License for Cisco 2901-2951	1
SL-29-SEC-K9	SL-29-SEC-K9	Cisco	Security License for Cisco 2901-2951	1
SM-DSK-SATA-500GB	SM-DSK-SATA-500GB	Cisco	500 GB hard disk drive for SRE SM	2
SM-MEM-VLP-2GB	SM-MEM-VLP-2GB	Cisco	2GB Very Low Profile SDRAM for SRE SM	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-2921SEC	CON-SNT-2921SEC	Cisco	SMARTNET 8X5XNBD Cisco 2921 Security	1
DISK-MODE-RAID-0	DISK-MODE-RAID-0	Cisco	Configure hard drives as RAID 0	1
FL-VMSS-SM-MS	FL-VMSS-SM-MS	Cisco	Video Management and Storage System Media Server License	1
FL-VMSS-SM-OM	FL-VMSS-SM-OM	Cisco	Video Management and Storage System Operations Manager Licen	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
MEM-2900-512U2.5GB	MEM-2900-512U2.5GB	Cisco	512MB to 2.5GB DRAM Upgrade (2GB+512MB) for Cisco 2901-2921	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
S29UK9-15102T	S29UK9-15102T	Cisco	Cisco 2901-2921 IOS UNIVERSAL	1
SM-SRE-900-K9	SM-SRE-900-K9	Cisco	Services Module with Services Ready Engine (SRE)	1
SM-VMSS-6.2.1-K9	SM-VMSS-6.2.1-K9	Cisco	Video Management and Storage System Software 6.2.1for the SM	1
SM9-VMSS	SM9-VMSS	Cisco	VMSS software contrainer for SM-SRE-900-K9	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1

CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	1
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	1
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	1
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	1
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	1
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	1
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	1
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	1

CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	1
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C2960S-48FPS-L	WS-C2960S-48FPS-L	Cisco	Cisco Catalyst 2960S 48 GigE PoE 740W, 4 x SFP LAN Base	1
CAB-L620P-C13-US	CAB-L620P-C13-US	Cisco	Power Cord, 250VAC, 15A, NEMA L6-20 to C13, US	1

Branches—Medium Branch

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502E-A-K9	AIR-CAP3502E-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Ext Ant; A Reg Domain	7
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	7
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	7
AIR-ANT2422DW-R	AIR-ANT2422DW-R	Cisco	2.4 GHz 2.2 dBi Swivel Dipole Antenna White, RP-TNC	21
AIR-ANT5135DW-R	AIR-ANT5135DW-R	Cisco	5 GHz 3.5 dBi Swivel Dipole Antenna White, RP-TNC	21
CON-SNT-CAP3502A	CON-SNT-CAP3502A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; E	7
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	7
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	7
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	7
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	7
CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	7
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	7
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4

CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CISCO2951-SEC/K9	CISCO2951-SEC/K9	Cisco	Cisco 2951 Security Bundle w/SEC license PAK	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-2921-51-AC	PWR-2921-51-AC	Cisco	Cisco 2921/2951 AC Power Supply	1
SL-29-IPB-K9	SL-29-IPB-K9	Cisco	IP Base License for Cisco 2901-2951	1
SL-29-SEC-K9	SL-29-SEC-K9	Cisco	Security License for Cisco 2901-2951	1
SM-DSK-SATA-500GB	SM-DSK-SATA-500GB	Cisco	500 GB hard disk drive for SRE SM	2
SM-MEM-VLP-2GB	SM-MEM-VLP-2GB	Cisco	2GB Very Low Profile SDRAM for SRE SM	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
DISK-MODE-RAID-0	DISK-MODE-RAID-0	Cisco	Configure hard drives as RAID 0	1
FL-VMSS-SM-MS	FL-VMSS-SM-MS	Cisco	Video Management and Storage System Media Server License	1
FL-VMSS-SM-OM	FL-VMSS-SM-OM	Cisco	Video Management and Storage System Operations Manager Licen	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
MEM-2951-512U2GB	MEM-2951-512U2GB	Cisco	512MB to 2GB DRAM Upgrade (1 2GB DIMM) for Cisco 2951 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
S2951UK9-15102T	S2951UK9-15102T	Cisco	Cisco 2951 IOS UNIVERSAL	1
SM-SRE-900-K9	SM-SRE-900-K9	Cisco	Services Module with Services Ready Engine (SRE)	1
SM-VMSS-6.2.1-K9	SM-VMSS-6.2.1-K9	Cisco	Video Management and Storage System Software 6.2.1for the SM	1
SM9-VMSS	SM9-VMSS	Cisco	VMSS software contrainer for SM-SRE-900-K9	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CISCO2951-SEC/K9	CISCO2951-SEC/K9	Cisco	Cisco 2951 Security Bundle w/SEC license PAK	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-2921-51-AC	PWR-2921-51-AC	Cisco	Cisco 2921/2951 AC Power Supply	1

SL-29-IPB-K9	SL-29-IPB-K9	Cisco	IP Base License for Cisco 2901-2951	1
SL-29-SEC-K9	SL-29-SEC-K9	Cisco	Security License for Cisco 2901-2951	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
MEM-2951-512U2GB	MEM-2951-512U2GB	Cisco	512MB to 2GB DRAM Upgrade (1 2GB DIMM) for Cisco 2951 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
NME-AIR-WLC25-K9	NME-AIR-WLC25-K9	Cisco	25-AP WLAN Controller NM for Cisco 2800/3800 Series	1
S2951UK9-15102T	S2951UK9-15102T	Cisco	Cisco 2951 IOS UNIVERSAL	1
SM-NM-ADPTR	SM-NM-ADPTR	Cisco	Network Module Adapter for SM Slot on Cisco 2900, 3900 ISR	1
SWLCEK9-60	SWLCEK9-60	Cisco	Cisco Unified WLAN Controller SW Release 6.0 - MD	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	2
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	2
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	2
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	2
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	2
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	2
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	2
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	2
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	2
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1

CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	2
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	2
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	2
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	2
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	2
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	2
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	2
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	2
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	2
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	1
CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	1
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C2960PD-8TT-L	WS-C2960PD-8TT-L	Cisco	Cisco Catalyst 2960 Powered Device 8 10/100 + 1 1000BT LAN Base	10
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	10
CON-SNT-C2960P8T	CON-SNT-C2960P8T	Cisco	SMARTNET 8X5XNBD Cat2960 Pwrd Device 8 10/100-1 1K BT LAN	10
PWR-A	PWR-A	Cisco	Pwr Sply In:100-240VAC Out:48VDC 380mA-2960PD-8TT-L	10
WS-C3750X-48PF-S	WS-C3750X-48PF-S	Cisco	Cisco Catalyst 3750X 48 Port Full PoE IP Base	2
C3KX-PWR-1100WAC	C3KX-PWR-1100WAC	Cisco	Cisco Catalyst 3K-X 1100W AC Power Supply	2
C3KX-NM-1G	C3KX-NM-1G	Cisco	Cisco Catalyst 3K-X 1G Network Module option PID	2

C3KX-PWR-1100WAC/2	C3KX-PWR-1100WAC/2	Cisco	Cisco Catalyst 3K-X 1100W AC Secondary Power Supply	2
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	4
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	2
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	2
CON-SNT-3750X4FS	CON-SNT-3750X4FS	Cisco	SMARTNET 8X5XNBD Catalyst 3750X 48 Port Full PoE IP Base	2
S375XVK9T-12253SE	S375XVK9T-12253SE	Cisco	Cisco CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	2
SFP-GE-S=	SFP-GE-S=	Cisco	1000BASE-SX SFP (DOM)	8

Branches—Large Branch

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502E-A-K9	AIR-CAP3502E-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Ext Ant; A Reg Domain	12
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	12
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	12
AIR-ANT2422DW-R	AIR-ANT2422DW-R	Cisco	2.4 GHz 2.2 dBi Swivel Dipole Antenna White, RP-TNC	36
AIR-ANT5135DW-R	AIR-ANT5135DW-R	Cisco	5 GHz 3.5 dBi Swivel Dipole Antenna White, RP-TNC	36
CON-SNT-CAP3502A	CON-SNT-CAP3502A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; E	12
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	12
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	12
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	12
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	12
CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	12
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	12

AIR-CT5508-25-K9	AIR-CT5508-25-K9	Cisco	Cisco 5508 Series Wireless Controller for up to 25 APs	2
LIC-CT5508-25	LIC-CT5508-25	Cisco	25 AP Base license	2
LIC-CT5508-BASE	LIC-CT5508-BASE	Cisco	Base Software License	2
AIR-PWR-5500-AC	AIR-PWR-5500-AC	Cisco	Cisco 5500 Series Wireless Controller Redundant Power Supply	2
AIR-PWR-CORD-NA	AIR-PWR-CORD-NA	Cisco	AIR Line Cord North America	4
CON-SNT-CT0825	CON-SNT-CT0825	Cisco	SMARTNET 8X5XNBD Cisco 5508 Series	2
GLC-T=	GLC-T=	Cisco	1000BASE-T SFP	6
SWC5500K9-70	SWC5500K9-70	Cisco	Cisco Unified Wireless Controller SW Release 7.0	2
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	8
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	8
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	8
CISCO3945-SEC/K9	CISCO3945-SEC/K9	Cisco	Cisco 3945 Security Bundle w/SEC license PAK	1
3900-FANASSY	3900-FANASSY	Cisco	Cisco 3925/3945 Fan Assembly (Bezel included)	1
C3900-SPE150/K9	C3900-SPE150/K9	Cisco	Cisco Services Performance Engine 150 for Cisco 3945 ISR	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-3900-AC	PWR-3900-AC	Cisco	Cisco 3925/3945 AC Power Supply	1
SL-39-IPB-K9	SL-39-IPB-K9	Cisco	IP Base License for Cisco 3925/3945	1
SL-39-SEC-K9	SL-39-SEC-K9	Cisco	Security License for Cisco 3900 Series	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2
CON-P2ST-NMEIPSK9	CON-P2ST-NMEIPSK9	Cisco	PM2, 8X5XNBD NME-IPS-K9	1
CON-SNT-3945SEC	CON-SNT-3945SEC	Cisco	SMARTNET 8X5XNBD Cisco 3945 Security Bundle w/SEC license	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
IPS-SW-NME-7.0-K9	IPS-SW-NME-7.0-K9	Cisco	IPS Software v7.0 for NME-IPS	1
MEM-3900-1GU2GB	MEM-3900-1GU2GB	Cisco	1GB to 2GB DRAM Upgrade (1GB+1GB) for Cisco 3925/3945 ISR	1

MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
NME-IPS-K9	NME-IPS-K9	Cisco	Cisco IPS NM for 2811, 2821, 2851 and 3800	1
PWR-3900-AC/2	PWR-3900-AC/2	Cisco	Cisco 3925/3945 AC Power Supply (Secondary PS)	1
S39UK9-15102T	S39UK9-15102T	Cisco	Cisco 3925-3945 IOS UNIVERSAL	1
SM-NM-ADPTR	SM-NM-ADPTR	Cisco	Network Module Adapter for SM Slot on Cisco 2900, 3900 ISR	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CISCO3945-SEC/K9	CISCO3945-SEC/K9	Cisco	Cisco 3945 Security Bundle w/SEC license PAK	1
3900-FANASSY	3900-FANASSY	Cisco	Cisco 3925/3945 Fan Assembly (Bezel included)	1
C3900-SPE150/K9	C3900-SPE150/K9	Cisco	Cisco Services Performance Engine 150 for Cisco 3945 ISR	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-3900-AC	PWR-3900-AC	Cisco	Cisco 3925/3945 AC Power Supply	1
SL-39-IPB-K9	SL-39-IPB-K9	Cisco	IP Base License for Cisco 3925/3945	1
SL-39-SEC-K9	SL-39-SEC-K9	Cisco	Security License for Cisco 3900 Series	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2
CON-P2ST-NMEIPSK9	CON-P2ST-NMEIPSK9	Cisco	PM2, 8X5XNBD NME-IPS-K9	1
CON-SNT-3945SEC	CON-SNT-3945SEC	Cisco	SMARTNET 8X5XNBD Cisco 3945 Security Bundle w/SEC license	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
IPS-SW-NME-7.0-K9	IPS-SW-NME-7.0-K9	Cisco	IPS Software v7.0 for NME-IPS	1
MEM-3900-1GU2GB	MEM-3900-1GU2GB	Cisco	1GB to 2GB DRAM Upgrade (1GB+1GB) for Cisco 3925/3945 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
NME-IPS-K9	NME-IPS-K9	Cisco	Cisco IPS NM for 2811, 2821, 2851 and 3800	1
PWR-3900-AC/2	PWR-3900-AC/2	Cisco	Cisco 3925/3945 AC Power Supply (Secondary PS)	1

S39UK9-15102T	S39UK9-15102T	Cisco	Cisco 3925-3945 IOS UNIVERSAL	1
SM-NM-ADPTR	SM-NM-ADPTR	Cisco	Network Module Adapter for SM Slot on Cisco 2900, 3900 ISR	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	4
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	4
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	4
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	4
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	4
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	4
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	4
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	4
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	4

CIVS-MSP-2RU	CIVS-MSP-2RU	Cisco	2RU w/Motherboard;1 CPU;RAID;Pwr Supp;NO Drives;NO Options	1
CIVS-CAB-16-AC	CIVS-CAB-16-AC	Cisco	CIVS C16 Power Cable North America	2
CIVS-HDD-1000	CIVS-HDD-1000	Cisco	1TB SATA Drive for CIVS-MSP	12
CIVS-MS-SW6.2	CIVS-MS-SW6.2	Cisco	CIVS-MS Media Server v6.2 Software License with Hardware	1
CIVS-PS-900	CIVS-PS-900	Cisco	Redundant 900W Power Supply for CIVS-MSP 2RU, 4RU	1
CIVS-VSM-SW4262	CIVS-VSM-SW4262	Cisco	CIVS-VSM Video Surveillance Manager v4.2/6.2 SW Mfg Image	1
CON-SNT-VSM2U	CON-SNT-VSM2U	Cisco	SMARTNET 8X5XNBD 2RU MSP Assembly	1
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	2
CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	2
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C3560-8PC-S	WS-C3560-8PC-S	Cisco	Catalyst 3560 Compact 8 10/100 PoE + 1 T/SFP; IP Base Image	20
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	20
CON-SNTP-WSC3568	CON-SNTP-WSC3568	Cisco	SMARTNET 24X7X4 Catalyst 3560 8 10/1	20
WS-C3560X-24P-S	WS-C3560X-24P-S	Cisco	Cisco Catalyst 3560X 24 Port PoE IP Base	6
C3KX-PWR-715WAC	C3KX-PWR-715WAC	Cisco	Cisco Catalyst 3K-X 715W AC Power Supply	6
C3KX-NM-1G	C3KX-NM-1G	Cisco	Cisco Catalyst 3K-X 1G Network Module option PID	6
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	6
CON-SNT-3560X2PS	CON-SNT-3560X2PS	Cisco	SMARTNET 8X5XNBD Catalyst 3560X 24 Port PoE IP Base	6
S356XVK9T-12253SE	S356XVK9T-12253SE	Cisco	CAT 3560X IOS UNIVERSAL WITH WEB BASED DEV MGR	6
SFP-GE-S=	SFP-GE-S=	Cisco	1000BASE-SX SFP (DOM)	12

WS-C4507R+E	WS-C4507R+E	Cisco	Cisco Catalyst 4500E 7 slot chassis for 48Gbps/slot	2
C4500E-IPB	C4500E-IPB	Cisco	Paper IP Base License	2
CAB-AC-2800W-TWLK	CAB-AC-2800W-TWLK	Cisco	U.S. Power Cord, Twist Lock, NEMA 6-20 Plug	4
CON-SNT-C4507R+E	CON-SNT-C4507R+E	Cisco	SMARTNET 8X5XNBD Catalyst4500E 7 slot chassis for 48Gbps	2
GLC-SX-MM=	GLC-SX-MM=	Cisco	GE SFP, LC connector SX transceiver	48
PWR-C45-2800ACV	PWR-C45-2800ACV	Cisco	Cisco Catalyst 4500 2800W AC Power Supply (Data and PoE)	2
PWR-C45-2800ACV/2	PWR-C45-2800ACV/2	Cisco	Cisco Catalyst 4500 2800W AC Power Supply (Data and PoE)	2
S45UK9-31-01XO	S45UK9-31-01XO	Cisco	CAT4500e SUP7e Universal Crypto Image	2
WS-X4448-GB-SFP	WS-X4448-GB-SFP	Cisco	Cisco Catalyst 4500 48-Port 1000Base-X (SFPs Optional)	2
WS-X45-SUP7-E	WS-X45-SUP7-E	Cisco	Cisco Catalyst 4500 E-Series Supervisor, 848Gbps	2
WS-X45-SUP7-E/2	WS-X45-SUP7-E/2	Cisco	Cisco Catalyst 4500 E-Series Supervisor, 848Gbps	2
WS-X4624-SFP-E	WS-X4624-SFP-E	Cisco	Cisco Catalyst 4500 E-Series 24-Port GE (SFP)	2
WS-X4748-RJ45V+E	WS-X4748-RJ45V+E	Cisco	Cisco Catalyst 4500E 48-Port PoE 802.3at 10/100/1000(RJ45)	2

Data Center, Internet Edge, DMZ

Name	Catalog Num	Vendor	Description	Qty
ASA5585-S60-2A-K9	ASA5585-S60-2A-K9	Cisco	Cisco ASA 5585-X Chas w/ SSP60,6 GE,4 SFP+,2 GE Mgt,2 AC,3DES/AES	2
ASA-SSP-60-INC	ASA-SSP-60-INC	Cisco	Cisco ASA 5585-X Security Services Processor-60 with 6GE, 4SFP+	2
ASA-VPN-CLNT-K9	ASA-VPN-CLNT-K9	Cisco	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	Cisco ASA 5500 Strong Encryption License (3DES/AES)	2
ASA5585-BLANK-F	ASA5585-BLANK-F	Cisco	Cisco ASA 5585-X Full Width Blank Slot Cover	2
ASA5585-BLANK-HD	ASA5585-BLANK-HD	Cisco	Cisco ASA 5585-X Hard Drive Blank Slot Cover	4

ASA5585-PWR-AC	ASA5585-PWR-AC	Cisco	Cisco ASA 5585-X AC Power Supply	4
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	Cisco ASA 5500 Advanced Endpoint Assessment License for SSL VPN	2
ASA5500-SC-10	ASA5500-SC-10	Cisco	Cisco ASA 5500 10 Security Contexts License	2
ASA5500-SSL-1000	ASA5500-SSL-1000	Cisco	Cisco ASA 5500 SSL VPN 1000 Premium User License	2
CAB-US515P-C19-US	CAB-US515P-C19-US	Cisco	NEMA 5-15 to IEC-C19 13ft US	4
CON-SNT-A85S62K9	CON-SNT-A85S62K9	Cisco	SMARTNET 8X5XNBD ASA 5585-X Chas w/ SSP40,6 GE,4 SFP+,2 G	2
SF-ASA5585-8.2-K8	SF-ASA5585-8.2-K8	Cisco	Cisco ASA 5500 Series Software Version 8.2 for ASA 5585-X, DES	2
ASR1002-5G-SHA/K9	ASR1002-5G-SHA/K9	Cisco	Cisco ASR1002 Sec+HA Bundle w/ ESP-5G,AESK9,License,4GB DRAM	2
ASR1000-ESP5	ASR1000-ESP5	Cisco	Cisco ASR1K Embedded Services Processor,5Gbps,ASR1002 only	2
FLASR1-FPI-RTU	FLASR1-FPI-RTU	Cisco	Flex. Pack Insp. Right-To-Use Feat Lic,ASR1000 Series	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
FLASR1-IPSEC-RTU	FLASR1-IPSEC-RTU	Cisco	Encryption Right-To-Use Feature Lic for ASR1000 Series	2
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1002-PWR-AC	ASR1002-PWR-AC	Cisco	Cisco ASR1002 AC Power Supply	4
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	4
CON-SNTP-25GSHAK9	CON-SNTP-25GSHAK 9	Cisco	SMARTNET 24X7X4 ASR1002 Sec+HA Bundle w/ESP-5G, AESK9	2
ASR1004-20G-HA/K9	ASR1004-20G-HA/K9	Cisco	Cisco ASR1004 HA Bundle w/ ESP-20G,RP1,SIP10,AESK9,License	2
ASR1000-ESP20	ASR1000-ESP20	Cisco	Cisco ASR1000 Embedded Services Processor, 20G	2
ASR1000-SPA	ASR1000-SPA	Cisco	SPA for ASR1000; No Physical Part; For Tracking Only	4
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
M-ASR1K-HDD-40GB	M-ASR1K-HDD-40GB	Cisco	Cisco ASR1000 RP1 40GB HDD	2
M-ASR1K-RP1-4GB	M-ASR1K-RP1-4GB	Cisco	Cisco ASR1000 RP1 4GB DRAM	2

SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1000-RP1-BUN	ASR1000-RP1-BUN	Cisco	Cisco ASR1000 Route Processor 1, 4GB DRAM,Bundle Component	2
ASR1000-SIP10	ASR1000-SIP10	Cisco	Cisco ASR1000 SPA Interface Processor 10	2
ASR1000-SIP10-BUN	ASR1000-SIP10-BUN	Cisco	Cisco ASR1000 SPA Interface Processor 10, Bundle Component	2
ASR1004-PWR-AC	ASR1004-PWR-AC	Cisco	Cisco ASR1004 AC Power Supply	4
CAB-AC15A-90L-US	CAB-AC15A-90L-US	Cisco	15A AC Pwr Cord, left-angle (United States) (bundle option)	4
CON-SNTP-420GHAK9	CON-SNTP-420GHAK 9	Cisco	SMARTNET 24X7X4 ASR1004 Chassis 2 P/S	2
CON-SNTP-A1ESP20	CON-SNTP-A1ESP20	Cisco	SMARTNET 24X7X4 ASR1000 Embedded Svc Processor,20G,Crypt	2
CON-SNTP-ASRRP1B	CON-SNTP-ASRRP1B	Cisco	SMARTNET 24X7X4 Cisco ASR1000 Route Processor 1	2
CON-SNTP-ASRSIPB	CON-SNTP-ASRSIPB	Cisco	SMARTNET 24X7X4 Cisco ASR1000 SPA Interface Processor	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
SPA-1X10GE-L-V2	SPA-1X10GE-L-V2	Cisco	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter	4
XFP-10G-MM-SR	XFP-10G-MM-SR	Cisco	10GBASE-SR XFP Module	4
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
Ironport Bundle E-mail and Web	Ironport Bundle E-mail and Web	Cisco	Ironport A La Carte examples for Webn and E-mail	2
N5K-C5020P-NBF	N5K-C5020P-NBF	Cisco	Cisco Nexus 5020 NetApp OSM version, 2 PS	2
N5020-ACC-KIT	N5020-ACC-KIT	Cisco	Cisco Nexus 5020 Accessory Kit, Option	2
N5K-PAC-1200W	N5K-PAC-1200W	Cisco	Cisco Nexus 5020 PSU module, 100-240VAC 1200W	4
CAB-9K12A-NA	CAB-9K12A-NA	Cisco	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4

CON-SNTP-N5020	CON-SNTP-N5020	Cisco	SMARTNET 24X7X4 N5000 2RU Chassis no PS 5	2
N5000FMS1K9	N5000FMS1K9	Cisco	Cisco Nexus 5000 Fabric Manager Server License	2
N5K-M1600	N5K-M1600	Cisco	N5000 1000 Series Module 6port 10GE(req SFP+)	4
N5KUK9-421N2.1	N5KUK9-421N2.1	Cisco	Cisco Nexus 5000 Base OS Software Rel 4.2(1)N2(1)	2
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	16
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	64
WS-C3750X-24T-S	WS-C3750X-24T-S	Cisco	Cisco Catalyst 3750X 24 Port Data IP Base	6
C3KX-PWR-350WAC	C3KX-PWR-350WAC	Cisco	Cisco Catalyst 3K-X 350W AC Power Supply	6
S375XVK9T-12255SE	S375XVK9T-12255SE	Cisco	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	6
C3KX-PWR-350WAC/2	C3KX-PWR-350WAC/2	Cisco	Cisco Catalyst 3K-X 350W AC Secondary Power Supply	6
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	12
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	6
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	6
CON-SNTP-3750X2TS	CON-SNTP-3750X2TS	Cisco	SMARTNET 24X7X4 Catalyst 3750X 24 Port Data IP Base	6
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
WS-SVC-ASA-SM1-K9	WS-SVC-ASA-SM1-K9	Cisco	ASA Services Module for Catalyst 6500-E, 3DES/AES	1
SF-ASASM-8.5-K8	SF-ASASM-8.5-K8	Cisco	ASA Software 8.5 for Catalyst 6500-E ASASM, 2 free VFW	1
MEM-C6K-APP-24GB	MEM-C6K-APP-24GB	Cisco	Cat6500 24GB Service Module Memory	1
WS-SVC-ASA-SM1	WS-SVC-ASA-SM1	Cisco	Base ASA Services Module PID for K8/K9	1
SF-ASASM-ASDM-6.5	SF-ASASM-ASDM-6.5	Cisco	ASDM Software 6.5 for Catalyst 6500-E ASASM	1

ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
CON-OSP-ASASM9	CON-OSP-ASASM9	Cisco	ONSITE 24X7X4 ASA Service Module for Catalyst 6500-E	1
VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE30-MOD-K9	ACE30-MOD-K9	Cisco	Application Control Engine 30 Hardware	1
SC6K-A51-ACE	SC6K-A51-ACE	Cisco	ACE30 module Software Release 5(1)	1
ACE30-BASE-04-K9	ACE30-BASE-04-K9	Cisco	ACE30 Module with 4G, 1G Comp, 1K SSL TPS and 5VC	1
CON-OSP-ACE30MOD	CON-OSP-ACE30MO D	Cisco	ONSITE 24X7X4 Application Control Engine 30 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK 9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
WS-SVC-ASA-SM1-K9	WS-SVC-ASA-SM1-K 9	Cisco	ASA Services Module for Catalyst 6500-E, 3DES/AES	1
SF-ASASM-8.5-K8	SF-ASASM-8.5-K8	Cisco	ASA Software 8.5 for Catalyst 6500-E ASASM, 2 free VFW	1
MEM-C6K-APP-24GB	MEM-C6K-APP-24GB	Cisco	Cat6500 24GB Service Module Memory	1
WS-SVC-ASA-SM1	WS-SVC-ASA-SM1	Cisco	Base ASA Services Module PID for K8/K9	1
SF-ASASM-ASDM-6.5	SF-ASASM-ASDM-6.5	Cisco	ASDM Software 6.5 for Catalyst 6500-E ASASM	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1

CON-OSP-ASASM9	CON-OSP-ASASM9	Cisco	ONSITE 24X7X4 ASA Service Module for Catalyst 6500-E	1
SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cisco Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-ASA-SM1-K9	WS-SVC-ASA-SM1-K9	Cisco	ASA Services Module for Catalyst 6500-E, 3DES/AES	1
SF-ASASM-8.5-K8	SF-ASASM-8.5-K8	Cisco	ASA Software 8.5 for Catalyst 6500-E ASASM, 2 free VFW	1
MEM-C6K-APP-24GB	MEM-C6K-APP-24GB	Cisco	Cat6500 24GB Service Module Memory	1
WS-SVC-ASA-SM1	WS-SVC-ASA-SM1	Cisco	Base ASA Services Module PID for K8/K9	1
SF-ASASM-ASDM-6.5	SF-ASASM-ASDM-6.5	Cisco	ASDM Software 6.5 for Catalyst 6500-E ASASM	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
CON-OSP-ASASM9	CON-OSP-ASASM9	Cisco	ONSITE 24X7X4 ASA Service Module for Catalyst 6500-E	1
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K9	Cisco	600M IDSM-2 Mod for Cat	1
WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
WS-SVC-ASA-SM1-K9	WS-SVC-ASA-SM1-K9	Cisco	ASA Services Module for Catalyst 6500-E, 3DES/AES	1
SF-ASASM-8.5-K8	SF-ASASM-8.5-K8	Cisco	ASA Software 8.5 for Catalyst 6500-E ASASM, 2 free VFW	1

MEM-C6K-APP-24GB	MEM-C6K-APP-24GB	Cisco	Cat6500 24GB Service Module Memory	1
WS-SVC-ASA-SM1	WS-SVC-ASA-SM1	Cisco	Base ASA Services Module PID for K8/K9	1
SF-ASASM-ASDM-6.5	SF-ASASM-ASDM-6.5	Cisco	ASDM Software 6.5 for Catalyst 6500-E ASASM	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
CON-OSP-ASASM9	CON-OSP-ASASM9	Cisco	ONSITE 24X7X4 ASA Service Module for Catalyst 6500-E	1
VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE30-MOD-K9	ACE30-MOD-K9	Cisco	Application Control Engine 30 Hardware	1
SC6K-A51-ACE	SC6K-A51-ACE	Cisco	ACE30 module Software Release 5(1)	1
ACE30-BASE-04-K9	ACE30-BASE-04-K9	Cisco	ACE30 Module with 4G, 1G Comp, 1K SSL TPS and 5VC	1
CON-OSP-ACE30MOD	CON-OSP-ACE30MO D	Cisco	ONSITE 24X7X4 Application Control Engine 30 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK 9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1

WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K9	Cisco	600M IDSM-2 Mod for Cat	1
WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18

Data Center—WAN Aggregation

Name	Catalog Num	Vendor	Description	Qty
ASA5555-IPS-K9	ASA5555-IPS-K9	Cisco	ASA 5555-X with IPS, SW, 8GE Data, 1GE Mgmt, AC, 3DES/AES	1
ASA5500-SSL-10	ASA5500-SSL-10	Cisco	ASA 5500 SSL VPN 10 Premium User License	1
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	ASA 5500 Advanced Endpoint Assessment License for SSL VPN	1
ASA-AC-E-5555	ASA-AC-E-5555	Cisco	AnyConnect Essentials VPN License - ASA 5555-X (5000 Users)	1
ASA-VPNP-5555	ASA-VPNP-5555	Cisco	Premium Shared VPN Participant License - ASA 5555-X	1
ASA-AC-M-5555	ASA-AC-M-5555	Cisco	AnyConnect Mobile - ASA 5555-X (req. Essentials or Premium)	1
ASA5500-SC-5	ASA5500-SC-5	Cisco	ASA 5500 5 Security Contexts License	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
SF-ASA-9.1-K8	SF-ASA-9.1-K8	Cisco	ASA 5500 Series Software Ver. 9.1 for ASA 5512X--5555X, DES	1
SF-ASAIPS64-7.1-K9	SF-ASAIPS64-7.1-K9	Cisco	ASA 5500-X IPS Software 7.1 for IPS SSP	1
ASA5555-IPS-SSP	ASA5555-IPS-SSP	Cisco	ASA 5555-X IPS SSP License	1
ASA-PWR-AC	ASA-PWR-AC	Cisco	ASA 5545-X/5555-X AC Power Supply	1
ASA-PWR-BLANK	ASA-PWR-BLANK	Cisco	ASA 5545-X/5555-X Power Slot Blank Cover	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1

ASR1002-5G-SHA/K9	ASR1002-5G-SHA/K9	Cisco	Cisco ASR1002 Sec+HA Bundle w/ ESP-5G,AESK9,License,4GB DRAM	4
ASR1000-ESP5	ASR1000-ESP5	Cisco	Cisco ASR1K Embedded Services Processor,5Gbps,ASR1002 only	4
FLASR1-FPI-RTU	FLASR1-FPI-RTU	Cisco	Flex. Pack Insp. Right-To-Use Feat Lic,ASR1000 Series	4
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	4
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	4
FLASR1-IPSEC-RTU	FLASR1-IPSEC-RTU	Cisco	Encryption Right-To-Use Feature Lic for ASR1000 Series	4
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	4
ASR1002-PWR-AC	ASR1002-PWR-AC	Cisco	Cisco ASR1002 AC Power Supply	8
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	8
CON-SNTP-25GSHAK9	CON-SNTP-25GSHAK 9	Cisco	SMARTNET 24X7X4 ASR1002 Sec+HA Bundle w/ESP-5G, AESK9	4
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
IPS-4260-4GE-BP-K9	IPS-4260-4GE-BP-K9	Cisco	4260 Bundle with 4-Port Cu NIC	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CON-P2SP-4260-4G	CON-P2SP-4260-4G	Cisco	PM2, 24X7X4 IPS-4260-4GE-BP-K9	2
IPS-4260-PWR	IPS-4260-PWR	Cisco	Redundant power for 4260	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
IPS-SW-6.2	IPS-SW-6.2	Cisco	Cisco IPS Sensor software version 6.2	2
WS-C3750X-24T-S	WS-C3750X-24T-S	Cisco	Cisco Catalyst 3750X 24 Port Data IP Base	8

C3KX-PWR-350WAC	C3KX-PWR-350WAC	Cisco	Cisco Catalyst 3K-X 350W AC Power Supply	8
S375XVK9T-12255SE	S375XVK9T-12255SE	Cisco	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	8
C3KX-PWR-350WAC/2	C3KX-PWR-350WAC/2	Cisco	Cisco Catalyst 3K-X 350W AC Secondary Power Supply	8
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	16
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	8
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	8
CON-SNTP-3750X2TS	CON-SNTP-3750X2TS	Cisco	SMARTNET 24X7X4 Catalyst 3750X 24 Port Data IP Base	8

Data Center—Service

Name	Catalog Num	Vendor	Description	Qty
ASA5585-S60-2A-K9	ASA5585-S60-2A-K9	Cisco	ASA 5585-X Chas w/ SSP60,6 GE,4 SFP+,2 GE Mgt,2 AC,3DES/AES	2
ASA-SSP-60-INC	ASA-SSP-60-INC	Cisco	ASA 5585-X Security Services Processor-60 with 6GE, 4SFP+	2
ASA-VPN-CLNT-K9	ASA-VPN-CLNT-K9	Cisco	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	Cisco ASA 5500 Strong Encryption License (3DES/AES)	2
ASA5585-BLANK-F	ASA5585-BLANK-F	Cisco	Cisco ASA 5585-X Full Width Blank Slot Cover	2
ASA5585-BLANK-HD	ASA5585-BLANK-HD	Cisco	Cisco ASA 5585-X Hard Drive Blank Slot Cover	4
ASA5585-PWR-AC	ASA5585-PWR-AC	Cisco	Cisco ASA 5585-X AC Power Supply	4
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	Cisco ASA 5500 Advanced Endpoint Assessment License for SSL VPN	2
ASA5500-SC-10	ASA5500-SC-10	Cisco	Cisco ASA 5500 10 Security Contexts License	2
CAB-US515P-C19-US	CAB-US515P-C19-US	Cisco	NEMA 5-15 to IEC-C19 13ft US	4
CON-SNT-A85S62K9	CON-SNT-A85S62K9	Cisco	SMARTNET 8X5XNBD ASA 5585-X Chas w/ SSP40,6 GE,4 SFP+,2 G	2
SF-ASA5585-8.2-K8	SF-ASA5585-8.2-K8	Cisco	Cisco ASA 5500 Series Software Version 8.2 for ASA 5585-X, DES	2

CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
IPS4270-2X10GE-K9	IPS4270-2X10GE-K9	Cisco	IPS 4270-20 bundled with 2-port 10GE NIC	2
IPS-2X10GE-SR-INC	IPS-2X10GE-SR-INC	Cisco	2X10GE interface card included in 10GE 4270 bundle	2
CAB-US515P-C19-US	CAB-US515P-C19-US	Cisco	NEMA 5-15 to IEC-C19 13ft US	4
CON-P2ST-IPS42702	CON-P2ST-IPS42702	Cisco	PM2, 8X5XNBD IPS 4270-20 bundled	2
IPS-2SX-INT	IPS-2SX-INT	Cisco	2-port fiber interface for the 4260 and 4270	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
IPS-SW-7.0	IPS-SW-7.0	Cisco	Cisco IPS software version 7.0	2
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE-16G-LIC	ACE-16G-LIC	Cisco	ACE20 16Gbps License	1

ACE-SSL-05K-K9	ACE-SSL-05K-K9	Cisco	Application Control Engine SSL License, 5000 TPS	1
ACE-VIRT-020	ACE-VIRT-020	Cisco	Application Control Engine Virtualization 20 Contexts	1
ACE20-MOD-K9	ACE20-MOD-K9	Cisco	Application Control Engine 20 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK 9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1
CON-SNT-ACE20MOD	CON-SNT-ACE20MOD	Cisco	SMARTNET 8X5XNBD Application Control	1
CON-SNT-WS-FWM1K9	CON-SNT-WS-FWM1K 9	Cisco	8x5xNBD Svc, Firewall blade for Catalyst 6500	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SC6K-A23-ACE	SC6K-A23-ACE	Cisco	ACE Module Software A2(3)	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K9	Cisco	600M IDSM-2 Mod for Cat	1
WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1

VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE-16G-LIC	ACE-16G-LIC	Cisco	ACE20 16Gbps License	1
ACE-SSL-05K-K9	ACE-SSL-05K-K9	Cisco	Application Control Engine SSL License, 5000 TPS	1
ACE-VIRT-020	ACE-VIRT-020	Cisco	Application Control Engine Virtualization 20 Contexts	1
ACE20-MOD-K9	ACE20-MOD-K9	Cisco	Application Control Engine 20 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK 9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1
CON-SNT-ACE20MOD	CON-SNT-ACE20MOD	Cisco	SMARTNET 8X5XNBD Application Control	1
CON-SNT-WS-FWM1K9	CON-SNT-WS-FWM1K 9	Cisco	8x5xNBD Svc, Firewall blade for Catalyst 6500	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SC6K-A23-ACE	SC6K-A23-ACE	Cisco	ACE Module Software A2(3)	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K9	Cisco	600M IDSM-2 Mod for Cat	1

WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18

Data Center—Secure Storage

Name	Catalog Num	Vendor	Description	Qty
DS-C9509-2AK9	DS-C9509-2AK9	Cisco	MDS 9509 Base Config: Chassis, 2 Sup-2A, 2 3K AC PS	2
CAB-9K16A-US2	CAB-9K16A-US2	Cisco	Power Cord 250VAC 16A, US/Japan, Src Plug NEMA L6-20	4
CON-SNT-4848K	CON-SNT-4848K	Cisco	SMARTNET 8X5XNBD Host Optimized 8G FC	4
CON-SNT-9304K	CON-SNT-9304K	Cisco	SMARTNET 8X5XNBD MDS 9000 18-port FC and 4-port GE Module	2
CON-SNT-C9509U	CON-SNT-C9509U	Cisco	SMARTNET 8X5XNBD MDS 9509 Base Config: Chassis, 2 Sup-2A	2
DS-9509-KIT-EMC	DS-9509-KIT-EMC	Cisco	MDS 9509 Accessory Kit for EMC	2
DS-SFP-FC4G-SW	DS-SFP-FC4G-SW	Cisco	4 Gbps Fibre Channel-SW SFP, LC	36
DS-SFP-FC8G-SW	DS-SFP-FC8G-SW	Cisco	8 Gbps Fibre Channel SW SFP+, LC	192
DS-X9248-48K9	DS-X9248-48K9	Cisco	4/44-Port Host-Optimized 8-Gbps FC Module	4
DS-X9304-18K9	DS-X9304-18K9	Cisco	MDS 9000 18-port FC and 4-port GE Module	2
M9500ENT1K9	M9500ENT1K9	Cisco	Enterprise package license for 1 MDS9500 switch	2
M9500SSE1K9	M9500SSE1K9	Cisco	Storage Services Enabler: 1 ASM on 1 MDS9500	2
M95IOA184	M95IOA184	Cisco	Cisco I/O Accelerator License for MSM-18/4 on MDS 9500	2
M95S2K9-5.0.4	M95S2K9-5.0.4	Cisco	MDS 9500 Supervisor/Fabric-2, NX-OS Software Release 5.0(4)	2
SSI-M9K9-504	SSI-M9K9-504	Cisco	MDS SSI Image 5.0(4)	2

Data Center—Extranet Edge

Name	Catalog Num	Vendor	Description	Qty
ASA5555-IPS-K9	ASA5555-IPS-K9	Cisco	ASA 5555-X with IPS, SW, 8GE Data, 1GE Mgmt, AC, 3DES/AES	1
ASA5500-SSL-10	ASA5500-SSL-10	Cisco	ASA 5500 SSL VPN 10 Premium User License	1
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	ASA 5500 Advanced Endpoint Assessment License for SSL VPN	1
ASA-AC-E-5555	ASA-AC-E-5555	Cisco	AnyConnect Essentials VPN License - ASA 5555-X (5000 Users)	1
ASA-VPNP-5555	ASA-VPNP-5555	Cisco	Premium Shared VPN Participant License - ASA 5555-X	1
ASA-AC-M-5555	ASA-AC-M-5555	Cisco	AnyConnect Mobile - ASA 5555-X (req. Essentials or Premium)	1
ASA5500-SC-5	ASA5500-SC-5	Cisco	ASA 5500 5 Security Contexts License	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
SF-ASA-9.1-K8	SF-ASA-9.1-K8	Cisco	ASA 5500 Series Software Ver. 9.1 for ASA 5512X--5555X, DES	1
SF-ASAIPS64-7.1-K9	SF-ASAIPS64-7.1-K9	Cisco	ASA 5500-X IPS Software 7.1 for IPS SSP	1
ASA5555-IPS-SSP	ASA5555-IPS-SSP	Cisco	ASA 5555-X IPS SSP License	1
ASA-PWR-AC	ASA-PWR-AC	Cisco	ASA 5545-X/5555-X AC Power Supply	1
ASA-PWR-BLANK	ASA-PWR-BLANK	Cisco	ASA 5545-X/5555-X Power Slot Blank Cover	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
ASR1002-5G-SHA/K9	ASR1002-5G-SHA/K9	Cisco	Cisco ASR1002 Sec+HA Bundle w/ ESP-5G,AESK9,License,4GB DRAM	2
ASR1000-ESP5	ASR1000-ESP5	Cisco	Cisco ASR1K Embedded Services Processor,5Gbps,ASR1002 only	2
FLASR1-FPI-RTU	FLASR1-FPI-RTU	Cisco	Flex. Pack Insp. Right-To-Use Feat Lic,ASR1000 Series	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
FLASR1-IPSEC-RTU	FLASR1-IPSEC-RTU	Cisco	Encryption Right-To-Use Feature Lic for ASR1000 Series	2

SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1002-PWR-AC	ASR1002-PWR-AC	Cisco	Cisco ASR1002 AC Power Supply	4
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	4
CON-SNTP-25GSHAK9	CON-SNTP-25GSHAK 9	Cisco	SMARTNET 24X7X4 ASR1002 Sec+HA Bundle w/ESP-5G, AESK9	2
ASR1004-20G-HA/K9	ASR1004-20G-HA/K9	Cisco	ASR1004 HA Bundle w/ ESP-20G,RP1,SIP10,AESK9,License	2
ASR1000-ESP20	ASR1000-ESP20	Cisco	Cisco ASR1000 Embedded Services Processor, 20G	2
ASR1000-SPA	ASR1000-SPA	Cisco	SPA for ASR1000; No Physical Part; For Tracking Only	4
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
M-ASR1K-HDD-40GB	M-ASR1K-HDD-40GB	Cisco	Cisco ASR1000 RP1 40GB HDD	2
M-ASR1K-RP1-4GB	M-ASR1K-RP1-4GB	Cisco	Cisco ASR1000 RP1 4GB DRAM	2
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1000-RP1-BUN	ASR1000-RP1-BUN	Cisco	Cisco ASR1000 Route Processor 1, 4GB DRAM,Bundle Component	2
ASR1000-SIP10	ASR1000-SIP10	Cisco	Cisco ASR1000 SPA Interface Processor 10	2
ASR1000-SIP10-BUN	ASR1000-SIP10-BUN	Cisco	Cisco ASR1000 SPA Interface Processor 10, Bundle Component	2
ASR1004-PWR-AC	ASR1004-PWR-AC	Cisco	Cisco ASR1004 AC Power Supply	4
CAB-AC15A-90L-US	CAB-AC15A-90L-US	Cisco	15A AC Pwr Cord, left-angle (United States) (bundle option)	4
CON-SNTP-420GHAK9	CON-SNTP-420GHAK 9	Cisco	SMARTNET 24X7X4 ASR1004 Chassis 2 P/S	2
CON-SNTP-A1ESP20	CON-SNTP-A1ESP20	Cisco	SMARTNET 24X7X4 ASR1000 Embedded Svc Processor,20G,Crypt	2
CON-SNTP-ASRRP1B	CON-SNTP-ASRRP1B	Cisco	SMARTNET 24X7X4 Cisco ASR1000 Route Processor 1	2
CON-SNTP-ASRSIPB	CON-SNTP-ASRSIPB	Cisco	SMARTNET 24X7X4 Cisco ASR1000 SPA Interface Processor	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
SPA-1X10GE-L-V2	SPA-1X10GE-L-V2	Cisco	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter	4
XFP-10G-MM-SR	XFP-10G-MM-SR	Cisco	10GBASE-SR XFP Module	4

CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
IPS-4260-4GE-BP-K9	IPS-4260-4GE-BP-K9	Cisco	4260 Bundle with 4-Port Cu NIC	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CON-P2SP-4260-4G	CON-P2SP-4260-4G	Cisco	PM2, 24X7X4 IPS-4260-4GE-BP-K9	2
IPS-4260-PWR	IPS-4260-PWR	Cisco	Redundant power for 4260	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
IPS-SW-6.2	IPS-SW-6.2	Cisco	Cisco IPS Sensor software version 6.2	2
N5K-C5020P-NBF	N5K-C5020P-NBF	Cisco	Cisco Nexus 5020 NetApp OSM version, 2 PS	2
N5020-ACC-KIT	N5020-ACC-KIT	Cisco	Nexus 5020 Accessory Kit, Option	2
N5K-PAC-1200W	N5K-PAC-1200W	Cisco	Nexus 5020 PSU module, 100-240VAC 1200W	4
CAB-9K12A-NA	CAB-9K12A-NA	Cisco	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
CON-SNTP-N5020	CON-SNTP-N5020	Cisco	SMARTNET 24X7X4 N5000 2RU Chassis no PS 5	2
N5000FMS1K9	N5000FMS1K9	Cisco	Nexus 5000 Fabric Manager Server License	2
N5K-M1600	N5K-M1600	Cisco	N5000 1000 Series Module 6port 10GE(req SFP+)	4
N5KUK9-421N2.1	N5KUK9-421N2.1	Cisco	Nexus 5000 Base OS Software Rel 4.2(1)N2(1)	2
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	16
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	64
WS-C3750X-24T-S	WS-C3750X-24T-S	Cisco	Cisco Catalyst 3750X 24 Port Data IP Base	8
C3KX-PWR-350WAC	C3KX-PWR-350WAC	Cisco	Cisco Catalyst 3K-X 350W AC Power Supply	8

S375XVK9T-12255SE	S375XVK9T-12255SE	Cisco	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	8
C3KX-PWR-350WAC/2	C3KX-PWR-350WAC/2	Cisco	Cisco Catalyst 3K-X 350W AC Secondary Power Supply	8
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	16
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	8
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	8
CON-SNTP-3750X2TS	CON-SNTP-3750X2TS	Cisco	SMARTNET 24X7X4 Catalyst 3750X 24 Port Data IP Base	8

Data Center—Physical Security

Name	Catalog Num	Vendor	Description	Qty
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	8
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	8
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	8
CIAC-PAME-1125-K9	CIAC-PAME-1125-K9	Cisco	Cisco Physical Access Manager Appliance	4
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CIAC-SW-LNX-1.0-K9	CIAC-SW-LNX-1.0-K9	Cisco	Cisco PAM Appliance Software Version 1.0	4
CON-SNT-PAM1125	CON-SNT-PAM1125	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	4
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	4
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	4

CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	4
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	4
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	4
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	4
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	4
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	4
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	4
CIVS-MSP-4RU	CIVS-MSP-4RU	Cisco	4RU w/Motherboard;1 CPU;RAID;Pwr Suppl;NO Drives;NO Options	2
CIVS-CAB-16-AC	CIVS-CAB-16-AC	Cisco	CIVS C16 Power Cable North America	4
CIVS-FC-1P	CIVS-FC-1P	Cisco	1 Port FibreChannel Card for CIVS-MSP	2
CIVS-HDD-1000	CIVS-HDD-1000	Cisco	1TB SATA Drive for CIVS-MSP	48
CIVS-MS-SW6.2	CIVS-MS-SW6.2	Cisco	CIVS-MS Media Server v6.2 Software License with Hardware	2
CIVS-PS-900	CIVS-PS-900	Cisco	Redundant 900W Power Supply for CIVS-MSP 2RU, 4RU	2
CIVS-VSM-SW4262	CIVS-VSM-SW4262	Cisco	CIVS-VSM Video Surveillance Manager v4.2/6.2 SW Mfg Image	2
CON-SNT-VSM4U	CON-SNT-VSM4U	Cisco	SMARTNET 8X5XNBD 4RU MSP Assembly	2
CIVS-SS-4U-42000	CIVS-SS-4U-42000	Cisco	Cisco VS 4U Storage System with 42x1000GB drives	4
CON-SNT-VSS442K	CON-SNT-VSS442K	Cisco	SMARTNET 8X5XNBD CIVS-SS-4U-42000	4

CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	10
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1

Data Center—Wireless Systems

Name	Catalog Num	Vendor	Description	Qty
AIR-CT5508-500-2PK	AIR-CT5508-500-2PK	Cisco	2x AIR-CT5508-500-K9	2
AIR-PWR-CORD-NA	AIR-PWR-CORD-NA	Cisco	AIR Line Cord North America	4
LIC-CT5508-500	LIC-CT5508-500	Cisco	500 AP Base license	4
LIC-CT5508-BASE	LIC-CT5508-BASE	Cisco	Base Software License	4
SWC5500K9-70	SWC5500K9-70	Cisco	Cisco Unified Wireless Controller SW Release 7.0	4
AIR-CT5508-500-K9Z	AIR-CT5508-500-K9Z	Cisco	5508 Series Controller for up to 500 APs	4
CON-SNTP-AIRC552P	CON-SNTP-AIRC552P	Cisco	SMARTNET 24X7X4 Two 5508 Series Controller for up to 500	2
AIR-MSE-3355-K9	AIR-MSE-3355-K9	Cisco	MSE 3355 Hardware SKU	2
AIR-MSE-PAK	AIR-MSE-PAK	Cisco	Mobility Services Configurable PAK	2
AIR-PWR-CORD-NA	AIR-PWR-CORD-NA	Cisco	AIR Line Cord North America	2
AIR-WIPS-AP-2000	AIR-WIPS-AP-2000	Cisco	Cisco wIPS License, Supporting Cisco 2000 Monitor Mode APs	2
SWMSE3355K9-70	SWMSE3355K9-70	Cisco	Cisco 3355 Series Mobility Services Engine SW Release 7.0	2
WCS-CD-K9	WCS-CD-K9	Cisco	CD With Windows And Linux. No License.	4
WCS-ENT-PLUS-K9	WCS-ENT-PLUS-K9	Cisco	Family SKU for WCS Enterprise PLUS License Products	1
CON-SAU-WENTK9	CON-SAU-WENTK9	Cisco	SW APP SUPP + UPGR Family SKU for WCS E	1
WCS-ENT-PLUS-10000	WCS-ENT-PLUS-10000	Cisco	Cisco WCS Enterprise PLUS License for 10,000 APs, Win/Linux	1

Data Center—Management

Note Previous validation included ACS 4.2.1 on Windows as shown in the implementation section 5. Subsequent validation was achieved for the Cisco ACS 5.3 appliance and is the recommended product in this BOM.

Name	Catalog Num	Vendor	Description	Qty
CSACS-1121-K9	CSACS-1121-K9	Cisco	ACS 1121 Appliance With 5.x SW And Base license	2
CSACS-5-BASE-LIC	CSACS-5-BASE-LIC	Cisco	Cisco Secure ACS 5 Base License	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2
CON-SNTP-SACS1121	CON-SNTP-SACS1121	Cisco	SMARTNET 24X7X4 ACS 1121 Appliance With 5.1	2
CSACS-5-ADV-LIC	CSACS-5-ADV-LIC	Cisco	ACS 5 Security Group Access System License	2
CSACS-5.2-SW-K9	CSACS-5.2-SW-K9	Cisco	Config Option: ACS 5.2 Software Loaded On 1121	2
CSMPR-LIC-1000	CSMPR-LIC-1000	Cisco	Cisco Security Manager Pro - Incremental 1000 Device License	1
CON-P2S-CSMPRI1K	CON-P2S-CSMPRI1K	Cisco	PM2, SAS CSM Ent Pro -1K incr. dev license	1
CSMPR50-4.0-K9	CSMPR50-4.0-K9	Cisco	Cisco Security Manager 4.0 Professional w/ 50 Device License	1
CSMPR50-PAK4	CSMPR50-PAK4	Cisco	CS Mgr Enterprise Pro 50 - Secondary PAK	1
CON-CSSPS-CSMPR504	CON-CSSPS-CSMPR504	Cisco	SHARED SUPP SAS CS Mgr 4.0 Enterprise Pro 50 DeviceBase	1
CSMPR50-U-4.0-K9	CSMPR50-U-4.0-K9	Cisco	Cisco Security Manager 3.x to 4.0 Upgrade - PRO-50 License	1
CSMPR50-PAK4	CSMPR50-PAK4	Cisco	CS Mgr Enterprise Pro 50 - Secondary PAK	1
NAC3355-3500-K9	NAC3355-3500-K9	Cisco	NAC Appliance 3355 Server -max 3500 users	4
NAC3355-95-CAVACC	NAC3355-95-CAVACC	Cisco	NAC Appliance 3355-95 Cavium Accelerator	4
NAC3355-SVR	NAC3355-SVR	Cisco	NAC Appliance 3355 Server Hardware	4
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	8
CON-SNT-NAC535M	CON-SNT-NAC535M	Cisco	SMARTNET 8X5XNBD NAC3355-3500-K9	4

NAC-SVR-48-K9	NAC-SVR-48-K9	Cisco	NAC Appliance Server Release 4.8	4
NACMGR-M-STD-K9	NACMGR-M-STD-K9	Cisco	Cisco NAC Standard Manager for 20 servers	2
NAC3355	NAC3355	Cisco	NAC Appliance 3355 Manager Hardware	2
NAC3355-95-CAVACC	NAC3355-95-CAVACC	Cisco	NAC Appliance 3355-95 Cavium Accelerator	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CON-SNT-NAMSTDK9	CON-SNT-NAMSTDK9	Cisco	SMARTNET 8X5XNBD NACMGR-M-STD-K9	2
SPESMA-VC-BASE	SPESMA-VC-BASE	Cisco	EMC VoyenceControl Base	1
SP-PRODUCTS-TERMS	SP-PRODUCTS-TERM S	Cisco	Buyer Acceptance of SolutionsPlus Terms and Conditions	1
SPESMA-VC-LIC	SPESMA-VC-LIC	Cisco	EMC VoyenceControl License Card	1
SPESMA-VCMD-P	SPESMA-VCMD-P	Cisco	EMC VoyenceControl Prod Lic (RTU Lic per NOC/Data Ctr)	1
SPESMA-VCMD1-03	SPESMA-VCMD1-03	Cisco	EMC VoyenceControl Managed Tier 1 Device License: 1001-1500	1,200
SPESMA-VCMD2-03	SPESMA-VCMD2-03	Cisco	EMC VoyenceControl Managed Tier 2 Device License: 1001-1500	1,200
SPESMA-VCMD3-03	SPESMA-VCMD3-03	Cisco	EMC VoyenceControl Managed Tier 3 Device License: 1001-1500	1,200
SPESMA-VCO-LIC	SPESMA-VCO-LIC	Cisco	EMC Voyence PCI Advisor License Card	1
SPESMA-VCO-NA02	SPESMA-VCO-NA02	Cisco	EMC Voyence Network Advisor - Less Than 10,000 Devices	1
SPESMA-VCO-PCI	SPESMA-VCO-PCI	Cisco	EMC Voyence PCI Advisor	1

Data Center—Access, Aggregation

Name	Catalog Num	Vendor	Description	Qty
L-VLVSG-VNMC=	L-VLVSG-VNMC=	Cisco	Virtual Network Mgmt Center Base License for VSG eDelivery	1
CON-CSSPU-LVLVSG	CON-CSSPU-LVLVSG	Cisco	SHARED SUPP SAU Virtual Network Mgmt Center Base for VSG	1
CON-SAU-LVLVSG	CON-SAU-LVLVSG	Cisco	SW APP SUPP + UPGR Virtual Network Mgmt Center Base for VSG	1

L-VLVSG-VNMC-P1	L-VLVSG-VNMC-P1	Cisco	VSG and VNMC eDelivery CPU License Promo 1 Qty 32	32
N1K-C1010	N1K-C1010	Cisco	Cisco Nexus 1010 Virtual Services Appliance	1
A01-X0105	A01-X0105	Cisco	2.66GHz Xeon X5650 95W CPU/12MB cache/DDR3 1333MHz	2
CAB-C13-C14-JMPR	CAB-C13-C14-JMPR	Cisco	Recessed receptical AC power cord 27	1
N01-M304GB1	N01-M304GB1	Cisco	4GB DDR3-1333MHz RDIMM/PC3-10600/dual rank 1Gb DRAMs	4
N1K-VLCPU-32	N1K-VLCPU-32	Cisco	Nexus 1000V for Nexus 1010 Paper CPU License Qty 32	1
N2XX-ABPCI03	N2XX-ABPCI03	Cisco	Broadcom 5709 Quad Port 10/100/1Gb NIC w/TOE iSCSI	1
R200-BBLKD	R200-BBLKD	Cisco	HDD slot blanking panel for UCS C200 M1 Rack Servers	2
R200-BHTS1	R200-BHTS1	Cisco	CPU heat sink for UCS C200 M1 Rack Server	2
R200-D500GCSATA03	R200-D500GCSATA03	Cisco	Gen 2 500GB SATA 7.2K RPM 3.5in HDD/hot plug/C200 drive sled	2
R200-PCIBLKF1	R200-PCIBLKF1	Cisco	PCIe Full Height blanking panel for UCS C-Series Rack Server	1
R200-SASCBL-001	R200-SASCBL-001	Cisco	Internal SAS Cable for a base UCS C200 M1 Server	1
R2X0-ML002	R2X0-ML002	Cisco	LSI 1064E (4-port SAS 3.0G RAID 0, 1, 1E) Mezz Card	1
R2X0-PSU2-650W-SB	R2X0-PSU2-650W-SB	Cisco	650W power supply, w/added 5A Standby for UCS C200 or C210	1
R2XX-CMAG3-1032	R2XX-CMAG3-1032	Cisco	Cable Mgmt Arm for R2XX-G31032RAIL for C200/C210	1
R2XX-G31032RAIL	R2XX-G31032RAIL	Cisco	G3 shorter stronger Rail Kit for UCS 200, 210 Rack Servers	1
R2XX-PSUBLKP	R2XX-PSUBLKP	Cisco	Power supply unit blnking pnl for UCS 200 M1 or 210 M1	1
R2XX-RAID1	R2XX-RAID1	Cisco	Enable RAID 1 Setting	1
CAB-N5K6A-NA	CAB-N5K6A-NA	Cisco	Power Cord, 200/240V 6A North America	1
N1K-VLCPU-32=	N1K-VLCPU-32=	Cisco	Nexus 1000V Paper CPU License Qty 32 (1YR Min Service)	1
N1K-VLCPU-01	N1K-VLCPU-01	Cisco	Nexus 1000V Paper CPU License Qty 1	32
N5K-C5020P-NBF	N5K-C5020P-NBF	Cisco	Nexus 5020 NetApp OSM version, 2 PS	2
N5020-ACC-KIT	N5020-ACC-KIT	Cisco	Nexus 5020 Accessory Kit, Option	2

N5K-PAC-1200W	N5K-PAC-1200W	Cisco	Nexus 5020 PSU module, 100-240VAC 1200W	4
CAB-9K12A-NA	CAB-9K12A-NA	Cisco	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
CON-SNTP-N5020	CON-SNTP-N5020	Cisco	SMARTNET 24X7X4 N5000 2RU Chassis no PS 5	2
N5000FMS1K9	N5000FMS1K9	Cisco	Nexus 5000 Fabric Manager Server License	2
N5K-M1600	N5K-M1600	Cisco	N5000 1000 Series Module 6port 10GE(req SFP+)	4
N5KUK9-421N2.1	N5KUK9-421N2.1	Cisco	Nexus 5000 Base OS Software Rel 4.2(1)N2(1)	2
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	16
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	64
N7K-C7010-BUN-R	N7K-C7010-BUN-R	Cisco	Nexus 7010 Bundle (Chassis,(2)SUP1,(3)FAB1,(3)AC-6KW PSU)	2
N7K-AC-6.0KW	N7K-AC-6.0KW	Cisco	Nexus 7000 - 6.0KW AC Power Supply Module	6
N7K-C7010-FAB1-BUN	N7K-C7010-FAB1-BUN	Cisco	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	6
N7K-SUP1-BUN	N7K-SUP1-BUN	Cisco	Nexus 7000 - Supervisor 1, Includes External 8GB Flash	4
CAB-AC-2500W-US1	CAB-AC-2500W-US1	Cisco	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	12
CON-SNTP-C701BR	CON-SNTP-C701BR	Cisco	SMARTNET 24X7X4 Nexus 7010 Bundle	2
N7K-CPF-2GB	N7K-CPF-2GB	Cisco	Nexus Compact Flash Memory 2GB (Expansion Flash - Slot 0)	4
N7K-M132XP-12	N7K-M132XP-12	Cisco	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	6
N7K-M148GT-11	N7K-M148GT-11	Cisco	Nexus 7000 - 48 Port 10/100/1000, RJ-45	2
N7KS1K9-50	N7KS1K9-50	Cisco	Cisco NX-OS Release 5.0	2
SFP-10G-SR	SFP-10G-SR	Cisco	10GBASE-SR SFP Module	34
WS-C4948-10GE-S	WS-C4948-10GE-S	Cisco	Catalyst 4948, IPB s/w, 48*10/100/1000+2*10GE(X2), 1 AC p/s	2
PWR-C49-300AC	PWR-C49-300AC	Cisco	Catalyst 4948 300-Watt AC Power Supply	2
S49IPB-12253SG	S49IPB-12253SG	Cisco	Cisco CAT4900 IOS IP BASE W/O CRYPTO	2
CAB-US515-C15-US	CAB-US515-C15-US	Cisco	NEMA 5-15 to IEC-C15 8ft US	2

CON-SNT-C4948GES	CON-SNT-C4948GES	Cisco	SMARTNET 8X5XNBD 4948, IPB s/w 4810/100/1K 2 10GE	2
X2-10GB-SR=	X2-10GB-SR=	Cisco	10GBASE-SR X2 Module	4

Data Center—UCS

Name	Catalog Num	Vendor	Description	Qty
N20-Z0001	N20-Z0001	Cisco	Cisco Unified Computing System	1
N1K-VLEM-UCS-1	N1K-VLEM-UCS-1	Cisco	Nexus 1000V License PAK For 1 Virtual Ethernet Module On UCS	32
VMW-VS-ENTP-1A	VMW-VS-ENTP-1A	Cisco	VMware vSphere Enterprise Plus (1 CPU), 1yr support required	32
A01-X0100	A01-X0100	Cisco	3.33GHz Xeon X5680 130W CPU/12MB cache/DDR3 1333MHz	64
A03-D146GC2	A03-D146GC2	Cisco	146GB 6Gb SAS 15K RPM SFF HDD/hot plug/drive sled mounted	64
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	16
CAB-N5K6A-NA	CAB-N5K6A-NA	Cisco	Power Cord, 200/240V 6A North America	4
CON-ISV1-VCS1A	CON-ISV1-VCS1A	Cisco	ISV 24X7 VMware vCenter Server Std 1 Yr RQD	32
CON-ISV1-VLEMUCS	CON-ISV1-VLEMUCS	Cisco	ISV 24X7 Nexus 1000V License PAK For 1 Virtual Et	64
CON-ISV1-VSENTP1A	CON-ISV1-VSENTP1A	Cisco	ISV 24X7 VMware vSphere EntPlus1CPU 1Yr RQD	32
CON-ISV1-VSENTP3A	CON-ISV1-VSENTP3A	Cisco	ISV 24X7 VMware vSphere EntPlus1CPU 3Yr RQD	32
CON-UCS1-1E0440	CON-UCS1-1E0440	Cisco	UC SUPPORT 8X5XNBD 4PT 10GE/4PT 4Gb FC/ExpanMod 6100Series	2
CON-UCS1-1S6200	CON-UCS1-1S6200	Cisco	UC SUPPORT 8X5XNBD 6140XP 40PT Fabric Interconnect	2
CON-UCS1-2C6508	CON-UCS1-2C6508	Cisco	UC SUPPORT 8X5XNBD 5108 Blade Server Chassis	4
CON-UCS1-2Z0001	CON-UCS1-2Z0001	Cisco	UC SUPPORT 8X5XNBD Cisco Unified Computing System	1
CON-UCS1-B66251	CON-UCS1-B66251	Cisco	UC SUPPORT 8X5XNBD UCSB200 M2 Blade Svr w/o CPU Mem HDD Mez	32
DS-SFP-FC4G-SW	DS-SFP-FC4G-SW	Cisco	4 Gbps Fibre Channel-SW SFP, LC	32

N01-M308GB2-L	N01-M308GB2-L	Cisco	8GB DDR3-1333MHz RDIMM/PC3-10600/dual rank/Low Voltage	384
N01-UAC1	N01-UAC1	Cisco	Single phase AC power module for UCS 5108	4
N10-E0440	N10-E0440	Cisco	4-port 10 GE/4-port 4Gb FC/Expansion module/UCS 6100 Series	2
N10-L001	N10-L001	Cisco	UCS 6100 Series Fabric Interconnect 1 10GE port license	32
N10-MGT005	N10-MGT005	Cisco	UCS Manager v1.3	2
N10-PAC2-750W	N10-PAC2-750W	Cisco	750W power supply unit for UCS 6140XP/100-240VAC	4
N10-S6200	N10-S6200	Cisco	UCS 6140XP 40-port Fabric Interconnect/0 PSU/5 fans/no SFP+	2
N10-SACCB	N10-SACCB	Cisco	Accessory kit for UCS 6140XP Fabric Interconnect	2
N10-SBLKE	N10-SBLKE	Cisco	Expansion module slot blanking panel for UCS 6100 Series	2
N1K-CSK9-UCS-404	N1K-CSK9-UCS-404	Cisco	Nexus 1000V VSM Virtual Appliance Software On UCS	32
N1K-VLEM-UCS-1	N1K-VLEM-UCS-1	Cisco	Nexus 1000V License PAK For 1 Virtual Ethernet Module On UCS	32
N20-AC0002	N20-AC0002	Cisco	UCS M81KR Virtual Interface Card/PCIe/2-port 10Gb	32
N20-B6625-1	N20-B6625-1	Cisco	UCS B200 M2 Blade Server w/o CPU, memory, HDD, mezzanine	32
N20-BHTS1	N20-BHTS1	Cisco	CPU heat sink for UCS B200 Blade Server	64
N20-C6508	N20-C6508	Cisco	UCS 5108 Blade Server Chassis/0 PSU/8 fans/0 fabric extender	4
N20-FAN5	N20-FAN5	Cisco	Fan module for UCS 5108	32
N20-FW005	N20-FW005	Cisco	UCS 5108 Blade Server Chassis FW package	4
N20-I6584	N20-I6584	Cisco	UCS 2104XP Fabric Extender/4 external 10Gb ports	8
N20-PAC5-2500W	N20-PAC5-2500W	Cisco	2500W power supply unit for UCS 5108	16
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	32
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	96
UCS-VMW-N1K-BUN	UCS-VMW-N1K-BUN	Cisco	Bundle of VMware Ent Plus and Nexus 1K License	32

VMW-VCS-1A	VMW-VCS-1A	Cisco	VMware vCenter Server Standard, 1yr support required	32
VMW-VS-ENTP-3A	VMW-VS-ENTP-3A	Cisco	VMware vSphere Enterprise Plus (1 CPU), 3yr support required	32

Data Center—Core

Name	Catalog Num	Vendor	Description	Qty
N7K-C7010-BUN-R	N7K-C7010-BUN-R	Cisco	Nexus 7010 Bundle (Chassis,(2)SUP1,(3)FAB1,(3)AC-6KW PSU)	1
N7K-AC-6.0KW	N7K-AC-6.0KW	Cisco	Nexus 7000 - 6.0KW AC Power Supply Module	3
N7K-C7010-FAB1-BUN	N7K-C7010-FAB1-BUN	Cisco	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	3
N7K-SUP1-BUN	N7K-SUP1-BUN	Cisco	Nexus 7000 - Supervisor 1, Includes External 8GB Flash	2
CAB-AC-2500W-US1	CAB-AC-2500W-US1	Cisco	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	6
CON-SNTP-C701BR	CON-SNTP-C701BR	Cisco	SMARTNET 24X7X4 Nexus 7010 Bundle	1
N7K-M132XP-12	N7K-M132XP-12	Cisco	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	3
N7K-M148GT-11	N7K-M148GT-11	Cisco	Nexus 7000 - 48 Port 10/100/1000, RJ-45	1
N7KS1K9-50	N7KS1K9-50	Cisco	Cisco NX-OS Release 5.0	1
N7K-C7010-BUN-R	N7K-C7010-BUN-R	Cisco	Nexus 7010 Bundle (Chassis,(2)SUP1,(3)FAB1,(3)AC-6KW PSU)	1
N7K-AC-6.0KW	N7K-AC-6.0KW	Cisco	Nexus 7000 - 6.0KW AC Power Supply Module	3
N7K-C7010-FAB1-BUN	N7K-C7010-FAB1-BUN	Cisco	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	3
N7K-SUP1-BUN	N7K-SUP1-BUN	Cisco	Nexus 7000 - Supervisor 1, Includes External 8GB Flash	2
CAB-AC-2500W-US1	CAB-AC-2500W-US1	Cisco	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	6
CON-SNTP-C701BR	CON-SNTP-C701BR	Cisco	SMARTNET 24X7X4 Nexus 7010 Bundle	1
N7K-M132XP-12	N7K-M132XP-12	Cisco	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	3

N7K-M148GT-11	N7K-M148GT-11	Cisco	Nexus 7000 - 48 Port 10/100/1000, RJ-45	1
N7KS1K9-50	N7KS1K9-50	Cisco	Cisco NX-OS Release 5.0	1



APPENDIX B

Cisco Products and Software Versions

	Device DNS Name	Model	Current Software
Branches			
	FW-A2-MSP-1	ASA5515-x	asa900-129-smp-k8.bin
	R-A2-Conv-1	CISCO891W	c890-universalk9-mz.151-3.T.bin
	R-A2-Mini-1	CISCO1941W-A/K9	c1900-universalk9-mz.SPA.151-3.T.bin
	R-A2-Small-1	CISCO2921/K9	c2900-universalk9-mz.SPA.151-3.T.bin
	R-A2-Med-1	CISCO2951 (STARSCREAM Rev 1)	c2951-universalk9-mz.SPA.151-3.T.bin
	R-A2-Med-2	CISCO2951/K9	c2951-universalk9-mz.SPA.151-3.T.bin
	R-A2-Lrg-1	C3945-SPE150/K9	c3900-universalk9-mz.SPA.151-3.T.bin
	R-A2-Lrg-2	C3945-SPE150/K9	c3900-universalk9-mz.SPA.151-3.T.bin
Internet Edge			
	RIE-1	ASR-1002X	asr1002x-universalk9.03.08.00.S.153-1.S.SPA.bin
	RIE-2	ASR-1002X	asr1002x-universalk9.03.08.00.S.153-1.S.SPA.bin
	RIE-3	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXI5.bin
	RIE-3_ASASM	WS-SVC-ASA-SM1-K9	asa911-smp-k8.bin / asdm-711.bin
	RIE-3_IDSM	WS-SVC-IDSM-2	7.0(4)
	RIE-3_ACE	ACE30-MOD-K9	c6ace-t1k9-mz.A5_2_1.bin
	RIE-4	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXI5.bin
	RIE-4_ASASM	WS-SVC-ASA-SM1-K9	asa911-smp-k8.bin / asdm-711.bin
	RIE-4_IDSM	WS-SVC-IDSM-2	7.0(4)
	RIE-4_ACE	ACE30-MOD-K9	c6ace-t1k9-mz.A5_2_1.bin
	ASA-IE-1	ASA5540 w/SSM-40	asa841-k8.bin
	ASA-IE-2	ASA5540 w/SSM-CSC-10	asa841-k8.bin

	IRONPort	Ironport C670	v7.1.3-010
Data Center			
	RWAN-1	ASR-1002 (RP1)	asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin
	RWAN-2	ASR-1002 (RP1)	asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin
	ASA-WAN-1	ASA5515-X	asa911-smp-k8.bin / asdm-711.bin
	ASA-WAN-2	ASA5515-X	asa911-smp-k8.bin / asdm-711.bin
	RCORE-1	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RCORE-2	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RAGG-1	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-1_VDC1	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-1_VDC2	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-2	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-2_VDC1	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-2_VDC2	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	DC-ASA-1_Admin	ASA-5585	asa824-smp-k8.bin
	DC-ASA-1_VDC1	ASA-5585	asa824-smp-k8.bin
	DC-ASA-1_VDC2	ASA-5585	asa824-smp-k8.bin
	DC-ASA-2_Admin	ASA-5585	asa824-smp-k8.bin
	DC-ASA-2_VDC1	ASA-5585	asa824-smp-k8.bin
	DC-ASA-2_VDC2	ASA-5585	asa824-smp-k8.bin
	RSERV-1	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RSERV-1_IDSM	WS-SVC-IDSM-2	7.0(4)
	RSERV-1_ACE	ACE30-MOD-K9	c6ace-t1k9-mz.A5_2_1.bin
	RSERV-2	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RSERV-2_IDSM	WS-SVC-IDSM-2	7.0(4)
	RSERV-2_ACE	ACE30-MOD-K9	c6ace-t1k9-mz.A5_2_1.bin
Branches			
	S-A2-MSP-1	WS-C2960S-48FPD-L	c2960s-universalk9-mz.122-53.SE2.bin
	A-A2-MSP-1	AIR-CAP3502I	
	S-A2-Conv-1	WS-C2960PD-8TT-L	c2960-lanbasek9-mz.122-55.SE1.bin

	S-A2-Mini-1	WS-C2960G-8TC-L	c2960-lanbasek9-mz.122-50.SE4.bin
	S-A2-Mini-2	WS-C2960-8TC-L	c2960-lanbasek9-mz.122-50.SE4.bin
	A-A2-Mini-1	AIR-CAP3502E	
	S-A2-Small-1	WS-C2960S-48FPS-L	c2960s-universalk9-mz.122-53.SE1.bin
	S-A2-Small-2 (Stacked)	WS-C2960S-48FPS-L	c2960s-universalk9-mz.122-53.SE1.bin
	A-A2-Small-1	AIR-CAP3502I	
	S-A2-Med-1	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	S-A2-Med-2 (Stacked)	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	S-A2-Med-3	WS-C2960CPD-8PT-L	c2960c405-universalk9-mz.122-55.0.43.SK.bin
	A-A2-Med-1	AIR-CAP3502E	
	A-A2-Med-2	AIR-LAP1262N	
	S-A2-Lrg-1	WS-4507+R SUP-7	cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
	S-A2-Lrg-2	WS-4507+R SUP-7	cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
	S-A2-Lrg-3	WS-C3560X-48PF-S	c3560e-universalk9-mz.122-53.SE2.bin
	S-A2-Lrg-4	WS-C3560X-48PF-S	c3560e-universalk9-mz.122-53.SE2.bin
	S-A2-Lrg-5	WS-C3560CPD-8PT-L	c3560c405ex-universalk9-mz.122-55.0.44.SK.bin
	A-A2-Lrg-1	AIR-CAP3502E	
	A-A2-Lrg-2	AIR-CAP3502I	
	SLC-A2-Lrg-1	AIR-CT5508-12-K9	7.0.114.112
	WAVE-A2-Lrg-1	WAVE-547	
Data Center			
	SWAN-1/2	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	SWAN-3/4	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	SACCESS-1	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	SACCESS-2	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	SACCESS-3	Nexus5020 Chassis ("40x10GE/Supervisor")	n5000-uk9.5.0.3.N1.1b.bin
	SACCESS-4	Nexus5020 Chassis ("40x10GE/Supervisor")	n5000-uk9.5.0.3.N1.1b.bin
	SACCESS-5	WS-C3750X-48P	c3750e-universalk9-mz.122-53.SE2.bin
	F-UCS-1	UCS6120-Fabric	4.1(3)N2(1.3p)
	F-UCS-2	UCS6120-Fabric	4.1(3)N2(1.3p)
	MDS-DC-1	MDS 9506 ("Supervisor/Fabric-2")	m9500-sf2ek9-mzg.5.0.1a.bin.S4
	MDS-DC-2	MDS 9506 ("Supervisor/Fabric-2")	m9500-sf2ek9-mz.5.0.4.bin
	AW-DC-1	AIR-WLC5508-12	7.0.114.112

	AW-DC-2	AIR-WLC5508-12	7.0.114.112
	MSE-DC-1	MSE3550	7.0.200.125
	MSE-DC-2	MSE3550	7.0.200.125
	Nexus 1kv	Nexus 1kv	4.2(1)SV1(4)
	Nexus VSG	Nexus VSG	4.2(1)VSG1(1)
	Cisco ISE	Cisco Identity Service Engine	1.2
	WCS Manager	Cisco WCS Manager	7.0.171.107
	CS Manager	Cisco Security Manager	4.0.1
	CS ACS	Cisco Secure Access Control Server	Release 4.2(1) Build 15 Patch 3
	Cisco Prime LMS	Cisco Prime Lan Management Solution	version 4.2.2 with NCM/Pari
	Cisco UCS Manager	Cisco UCS Manager	1.3(1p)
	Cisco UCM	Cisco Unified Communications Manager	8.5.1.11001-3
	EMC UIM	EMC Unified Infrastructure Manager'	2.0.1.1.160
	EMC Unisphere	EMC Unisphere	1.0.50.1.0326
	RSA DPM	RSA Data Protection Manager	KM-3.1 / AM-6.1.SP3
	RSA enVision	RSA enVision	RSA enVision 4.0 , Revision 5
	RSA Authentication Manager	RSA Authentication Manager	7.1 Service Pack 2
	RSA Archer	RSA Archer	4.5.5
	HyTrust	HyTrust	2.2.1.14064
	VSOM	Cisco Video Surveliance Manager	6.3.1
	PAM	Cisco Physical Access Manager	1.2.0



APPENDIX C

Verizon Business Reference Architecture Report—Cisco PCI Solution

Based on PCI DSS v. 2.0 (01/24/2013)

Table of Contents

Contact Information 2

1. Executive Summary 2
   - Architecture Description 2
   - High Level Network Diagram 3
   - Quarterly Vulnerability Scans 4

2. Description of Scope of Work and Approach Taken 4
   - PCI DSS Version 4
   - Timeframe 4
   - Environment on which Assessment Focused 4
   - Network Segmentation 5
   - Exclusions 5
   - Wireless LANs and/or Wireless Applications 6
   - List of Individuals Interviewed 6

Build and Maintain a Secure Network 7
   - Protect Cardholder Data 36

Maintain a Vulnerability Management Program 50
   - Implement Strong Access Control Measures 62

Regularly Monitor and Test Networks 89

Maintain an Information Security Policy 120

Contact Information



Verizon Business Rob McIndoe Sr. Security Consultant CISSP, PCI QSA, PA-QSA, CISA, GSEC Robert.Mcindoe@verizon.com Aaron Reynolds Principal Security Consultant CISSP, PCI QSA Aaron.Reynolds@verizon.com	
Cisco Systems, Inc Christian Janoff Compliance Solutions Architect christian.janoff@cisco.com Bart McGlothin Compliance Solutions Architect bart.mcglothin@cisco.com	



1. Executive Summary

Architecture Description

Cisco Systems, Inc engaged Verizon Business to conduct a PCI reference architecture assessment of their "PCI Solution" designed architecture, based on the PCI DSS v2.0 standard. The architecture assessment against the PCI DSS v2.0 standard included a review of the Cisco Compliance Solution for PCI DSS 2.0 network architecture, configurations, security applications, and web management consoles.

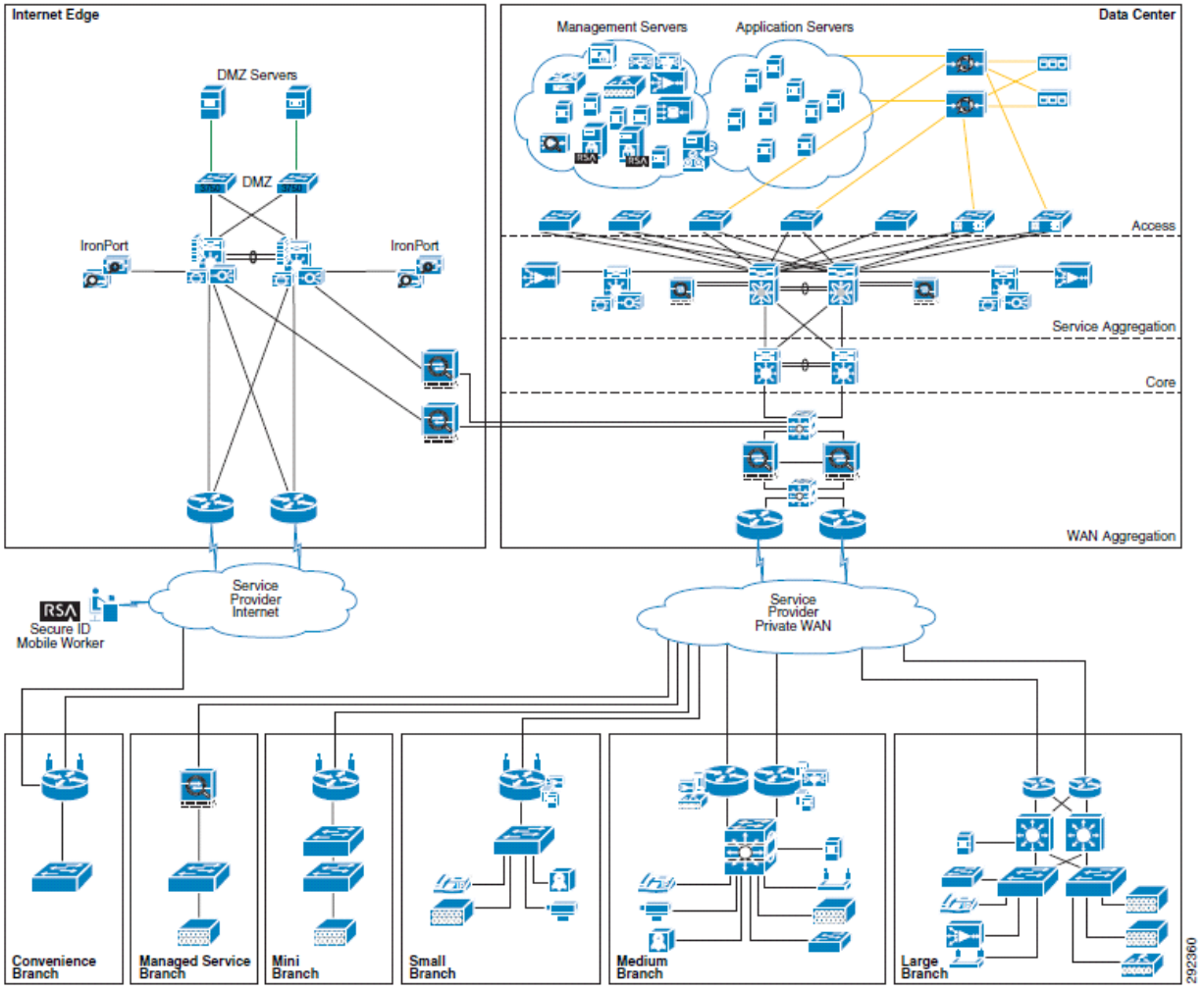
Cisco Systems, Inc. will continue to market the assessed reference architecture solution to customers looking to meet PCI requirements, specifically within their environment and within their back-end data center infrastructure. Cisco has used findings from the assessment to ensure configurations within their solution meet PCI requirements specific to their solution, and plan to provide the results of the assessment to Cisco Sales Engineers interfacing with enterprise customers.

Verizon Business' assessment covered PCI enterprise architectures, including: Datacenter, Internet Edge, WAN, and Branch architectures. In all, 6 branch designs were reviewed, which fall under small, medium, and large branch environments. Verizon Business found the solution architectures to address several technical PCI requirements, and can address other requirements either as a compensating control,

or in conjunction with compensating controls depending on organizations infrastructure requirements. The architectures are designed to be deployed within a POS location, with central management/logging components deployed in a data center environment.

As Cisco's PCI Solution architecture only addresses some aspects of an organization's overall PCI compliance responsibility, several areas of PCI compliance are left to the organization to obtain full compliance. The overall approach to the assessment was to focus validation efforts on components which are core to Cisco's PCI Solution environment. System components outside of the Cisco Compliance Solution for PCI environment (e.g. corporate email, corporate Internet/DMZ firewalls, central cardholder databases, POS systems, mainframes, and corporate networks) were not included in the scope of the assessment.

High Level Network Diagram



Quarterly Vulnerability Scans

N/A - Quarterly scanning (internal and external) is the responsibility of the organization/service provider, and was not part of the assessment.

2. Description of Scope of Work and Approach Taken

PCI DSS Version

PCI DSS v.2.0 was used for the current reference architecture review.

Timeframe

Verizon has performed multiple assessments of the Cisco PCI Solution for Retail. With each phase, additional infrastructure, technology, and supporting management applications have been added. The following is a brief summary of PCI-based assessments against the Cisco PCI Solution for Retail reference architecture:

- PCI DSS v1.1 (Phase I – 2006-2007)
- PCI DSS v1.1 (Phase II – 2007-2008)
- PCI DSS v1.2 (Phase III – 2008-2009)
- PCI DSS v2.0 (Phase IV – 2010-2011)
- PCI DSS v2.0 (Phase V (Current) – 2012-2013)

The current (Phase V) review took place through several remote interviews and remote validation:

- 10/4/2012 – 01/13/2013

Environment on which Assessment Focused (Phase IV & V)

The architecture assessment included the following components:

- **Cisco Routers** (ISR)—891w-AGN, 1941w, ISR G2, 2921/51 ISR G2, 3945 ISR G2, ASR1002, ISRs are configured with Firewall and IDS feature set.
- **Cisco Switches—**2960 PD-8TT-L, 2960- 8TC-L, 2960 S, 2960 C, 3560 C, 3560 X, 3750 X, 4507-Sup 7, 6500, Nexus1000v, Nexus5000, Nexus7000, MDS 9500
- MDS Switch Fabric
- **Cisco Wireless** —1262N Access Points, 3502E Access Points, 3502I Access Points, CT5508 Controller, WLC2125 Controller, Mobility Service Engine, WCS-Wireless Manager
- **Cisco Security devices—**ASA 5585, ASA 5555, ASA 5515-x, NAC, IOS Firewall, AnyConnect - VPN. Catalyst ASA Services Module, Catalyst Intrusion Detection Service Module
- **Server Vitalization—**Servers - ISR SRE 900, UCS Express server ESXi
- **VBlock—**UCS - MDS - EMC SAN
- **Cisco Security Manager—**Central provisioning of device configuration and security policies, including: ASAs, Cisco ASA Services Modules, IDS, ISRs, and switches

- **Cisco Secure Access Control Server** (ACS)—AAA server
- **Cisco Prime LAN Management Solution (LMS) –** Configuration Management / Configuration Enforcement and monitoring (Pari Compliance Module)
- **Cisco Identity Services Engine (ISE) -** Central Authentication, Policy / Configuration enforcement
- **RSA Access Manager—**Used for central authentication/logging for access to RSA Data Protection Manager within the assessed environment.
- **RSA Authentication Manager—**Central management/logging of RSA SecurID (two-factor) authentication for remote access into the data center environment.
- **RSA Data Protection Manager (**formerly RSA Key Manager**)**
- **RSA enVision—**RSA's solution for compliance and security information management. RSA enVision was used to centrally collect RSA SecurID authentication logs on the RSA Authentication Manager server, using a batch process that runs several times a day.
- **HyTrust—**Network-based virtual infrastructure policy enforcement. Administrative access control, enforcement of policy across virtual infrastructure, hypervisor hardening, and audit logging. Access and User administration, change and configuration, and operations

Network Segmentation

Cisco has designed several network architectures for small, medium, and large enterprise environments. Cisco has chosen Cisco Integrated Services Routers (ISRs) to provide firewall, IDS/, and routing functionality. Access-lists are applied through firewall policies, which are pushed to the ISRs in each architecture. Access-lists implicitly deny all inbound and outbound traffic to the PCI Solution; all traffic approved within each design is explicitly allowed to the IP address, port and service level. Additionally, Cisco has incorporated wireless into the design, using WPA-TKIP for secure wireless networking.

The data center environment is segmented into multiple VLANs, including Internet Edge, WAN aggregation, and Core service aggregation. Multiple layers of network security are included in all data center segments, including Cisco ASA Services Module and ASA stateful firewall filtering and integrated IDS/ detection/prevention, access lists, secure VPN (WAN aggregation and remote VPN), and two-factor authentication.

All network devices within the PCI Solution are centrally managed through the following:

- Cisco Security Manager (CSM) - (Central security management for ISRs and switches (e.g., firewall policy, IDS/signatures))
- Cisco Wireless Control System (WCS)—(Central wireless management)
- Cisco ACS—Central TACACS+ (central authentication) server for ASA firewall, Cisco ASA Services Module, ISR, ASR router, switch, wireless controller (RSA enVision and WCS).
- RSA enVision—Central logging/Correlation/Analysis/Alerting server. Alerts from IDS/alerts and firewall logs.
- Cisco ASDM—configuration for ASA firewalls.
- Cisco Device Manager (IDM)—IDS/configuration management.
- Cisco Prime LAN Management Solution (LMS)) – Central configuration management, monitoring, and troubleshooting.
- Cisco Identity Services Engine (ISE) – Central Authentication, Policy / Configuration enforcement for ASA firewall, Cisco ASASM, ISR / VXR routers, Cisco switch, and wireless controllers

Exclusions

Due to the nature of this assessment, several areas of a normal PCI assessment were excluded, including:

- Central cardholder data storage
- Authorization/settlement processes
- Policies, procedures, and standards
- Assessment of “in transit” cardholder data
- SDLC policies and procedures
- Live cardholder transactions (a POS environment, which includes authorization responses, was not available during the assessment)
- Vulnerability Scanning / Penetration Testing
- OS-layer system hardening (Windows servers)

Wireless LANs and/or Wireless Applications

Wireless networks within the PCI Solution environment have been configured to use WPA-TKIP authentication for secure wireless networking. All wireless traffic must pass through the ISRs and IOS firewall access-lists to traverse any part of the PCI Solution network. Additionally, best practice security parameters have been applied to wireless networks, including: HTTPS access for wireless management, default SSID has been changed, SNMPv3 used (default strings changed), and HTTP access has been disabled.

List of Individuals Interviewed

The following staff was interviewed:

Interviewee(s)	Title
Christian Janoff, Bart Mcglothin	Network architecture, firewalls, routers, switches, wireless, IDS/
Bart Mcglothin, Sai Balabhadrapatruni	ASA 9.0, Cisco IPS
Christian Janoff, Bart Mcglothin	Audit Logging
Christian Janoff, Bart Mcglothin	Access Control / Authentication
Christian Janoff, Bart Mcglothin, Raju Satyan	Cisco Prime LMS with Pari Compliance Module
Christian Janoff, Bart Mcglothin, Jamey Heary	Cisco ISE
Christian Janoff, Eric Vyncke	PCI and IPv6
Christian Janoff, Bart Mcglothin	CSM
Tom Hua	CSM
Christian Janoff, Bart Mcglothin	Wireless
Christian Janoff, Bart Mcglothin	LMS
Rupesh Chakkingal,	RSA Data Protection Manager
Rupesh Chakkingal	RSA Data Protection Manager

Bart Mcglothin	Cisco ASA – Secure configuration reviews
Sheri Spence	EMC SAN
Syed Ghayur	Nexus 1kv
Mike Adler	Wireless lab
Sujit Ghosh	Wireless lab
K. Sigel	HyTrust
R. Budko	HyTrust
Christian Janoff, Bart Mcglothin	Cisco Virtual Service Gateway
Syed Ghayur	Cisco Virtual Service Gateway
David Valiquette	RSA
Pandit Panburana	CUCM
Mourad Cherfaoui	CUCM
Danny Dhillon	RSA enVision
Danny Dhillon	RSA Authentication Manager
Danny Dhillon	RSA Data Protection Manager, RSA Access Manager, RSA Authentication Manager

List of Documents Reviewed

The following documents were reviewed:

Document	Date
Enterprise Retail PCI DSS 2.0.pdf	11/17/2010
switch and router configs	04/15/2011
Switch configs - branches	04/15/2011
Common requirements questions across all devices.xls	12/01/2010
Products Alignment_2010-10-13.xlsx	10/13/2010
PCI Retail Solution Products.xlsx	04/15/2011
ASA, router, ACE Load Balancer, and IPS configurations	11/12/2012
Compliance_LAB_Diagram_2012-12-03 - Internet Edge Page.pdf	12/06/2012
20121130 PCI DSS and IPv6.docx	11/30/2012
LMS and Pari_DIG Revision_2012-11-11.docx	11/12/2012
Lab_IP_Addressing_and_Consoles.xlsx	11/12/2012
Cisco ISE at a glance	11/30/2012
Cisco ISE Data Sheet	11/30/2012

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
1.1 Establish firewall and router configuration standards that include the following:	**1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.	**N/A** – Firewall/Router configuration standards (documentation) is the responsibility of the organization / service provider.		

1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram (for example, onethat shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.	Verizon Business reviewed network diagrams and verified that they document all connections to cardholder data, including any wireless networks.		**Note:** Since each network environment will be unique to the organization or service provider, updating network diagrams remains the responsibility of each organization / service provider
	1.1.2.b Verify that the diagram is kept current.	Verizon Business reviewed network diagrams and verified that they kept current.		**Note:** Since each network environment will be unique to the organization or service provider, updating network diagrams remains the responsibility of each organization / service provider
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3.a** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.	**N/A** – Firewall/Router configuration standards (documentation) is the responsibility of the organization / service provider.		
	1.1.3.b Verify that the current network diagram is consistent with the firewall configuration standards.	**N/A** – Firewall/Router configuration standards (documentation) is the responsibility of the organization / service provider.		

1.1.4 Description of groups, roles, and responsibilities for logical management of network components	**1.1.4** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.	**N/A** – Firewall/Router configuration standards (documentation) is the responsibility of the organization / service provider. **Note:** Verizon Business confirmed role-based groups were created within Cisco ISE & ACS for logical management of network devices (e.g. ERS Admin, ERS Guest, Helpdesk Admin, Policy Admin, System Admin, Network Device Admin, etc).		
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.	**1.1.5.a** Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.	**N/A** – Firewall/Router configuration standards (documentation) is the responsibility of the organization / service provider. **Note:** Verizon Business reviewed access-lists, in addition to a documented list of required services/protocols for the PCI Solution environment, and confirmed traffic is limited to that which is required for the environment.		
	1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service.	**N/A** – Firewall/Router configuration standards (documentation) is the responsibility of the organization / service provider.		

1.1.6 Requirement to review firewall and router rule sets at least every six months	**1.1.6.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.	**N/A** – Firewall/Router configuration standards (documentation) is the responsibility of the organization / service provider.		
	1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.	**N/A** – Firewall/Router configuration standards (documentation) is the responsibility of the organization / service provider.		
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. **Note:** An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	**1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:			

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	**1.2.1.a** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.	Verizon Business reviewed access lists across firewalls and routers and verified that inbound and outbound traffic is limited to that which is necessary for a cardholder data environment. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945		**Note:** Configurations for perimeter firewalls/routers outside the PCI Solution environment are the responsibility of organization / service provider.

	1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	Verizon Business reviewed access lists across firewalls and routers and verified that all other inbound and outbound traffic is specifically denied. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945		

1.2.2 Secure and synchronize router configuration files.	**1.2.2** Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.	Verizon Business reviewed router configuration and verified that configuration files are secure and synchronized. Verizon also observed Cisco Prime LMS provides configuration enforcement and monitoring, to ensure router configurations are running against secure configuration templates and that startup and running configurations are in sync. Verizon Business observed system-generated configuration output for the following system components: Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco Prime LMS Cisco ASA 5500 Series-branch (functioning as a router) Cisco ASA 5515-x		

1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	**1.2.3** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	Verizon Business confirmed that the PCI Reference Architecture Solutions was designed and segmented to require all wireless traffic destined for any wired host (WCS Manager), to pass through firewall access-lists before being permitted. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945		
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	**1.3** Examine firewall and router configurations—incl uding but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—to determine that there is no direct access between the Internet and system components in the internal cardholder network segment, as detailed below.			

1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**1.3.1** Verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Verizon Business reviewed network topologies and access lists across firewalls and routers and verified that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Services Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555		

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	**1.3.2** Verify that inbound Internet traffic is limited to IP addresses within the DMZ.	Verizon Business reviewed static IPs, and access lists across firewalls and routers and verified that that inbound Internet traffic is limited to IP addresses within the DMZ. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002		**Note;** Perimeter firewall/router configurations and rule sets are the responsibility of the organization / service provider.

1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	**1.3.3** Verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.	Verizon Business reviewed network diagrams, configurations from network-infrastructure system components, including wireless APs and verified that direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002		

1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	**1.3.4** Verify that internal addresses cannot pass from the Internet into the DMZ**.**	Verizon Business reviewed access-lists on the Internet edge router and confirmed that Internet sourced RFC-1918 addresses are explicitly denied and that internal addresses cannot pass from the Internet into the DMZ. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002		

1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**1.3.5** Verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized	Verizon Business reviewed outbound access-lists from the PCI Reference Architecture Solutions environment and confirmed that all outbound traffic is destined for "data center" systems. There is no outbound Internet access from the PCI Reference Architecture Solutions environment. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002		

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	**1.3.6** Verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.)	Verizon Business confirmed the PCI Solution environment configurations for the Cisco ASA firewalls, Cisco Virtual Service Gateways, Cisco Firewall Services Modules, and ISRs with a firewall feature set were configured to perform stateful packet inspections. Verizon Business observed system-generated configuration output for the following system components: Cisco routers-data center Cisco ASR 1002 Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002		

1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**1.3.7** Verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.	Verizon Business reviewed network topologies, network diagrams, and access lists across firewalls and routers and verified that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002		

1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. **Note:** Methods to obscure IP addressing may include, but are not limited to: • *Network Address Translation (NAT)* • *Placing servers containing cardholder data behind proxy servers/firewalls or content caches,* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* • *Internal use of RFC1918 address space instead of registered addresses.*	**1.3.8.a** Verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	Verizon Business reviewed DHCP reservations, static IPs, and access lists across firewalls and routers and confirmed that RFC 1918 addresses were used within the PCI Solution environment. Verizon also observed Cisco ASA, ACE SLB, and router configuration settings configured for IPv6 addressing. Verizon Business observed that internal, private IP addresses, whether IPv4 or IPv6 can be prevented from disclosure through one or more network design options, including: • Stateful NAT64 • Server Load Balanced IPv6-to-IPv4 (SLB64) • Outbound web proxy (e.g. for outbound Internet connections from IPv6 address to the Internet) Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002		

	1.3.8.b Verify that any disclosure of private IP addresses and routing information to external entities is authorized.	**N/A** – Policies and procedures is the responsibility of the organization / service provider.		
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	**1.4.a** Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active.	**N/A** – Security Policy (Remote Access – Desktop firewalls) is the responsibility of the organization / service provider. Installation of personal firewall software for any mobile and employee-owned computers with direct Internet connectivity, and which are used to access the organization / service provider network, is the responsibility of the organization / service provider.		
	1.4.b Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by users of mobile and/or employee-owned computers.	**N/A** – Security Policy (Remote Access – Desktop firewalls) is the responsibility of the organization / service provider. Installation of personal firewall software for any mobile and employee-owned computers with direct Internet connectivity, and which are used to access the organization / service provider network, is the responsibility of the organization / service provider.		

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
2.1 Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	**2.1** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords	Verizon Business observed administrators during the login process, while attempting to logon with default accounts and passwords. Verizon Business confirmed all default passwords, including passwords for interactive administrator accounts and SNMP community strings have been changed. Verizon Business confirmed all default administrator accounts have been removed, where possible. Some default administrator accounts cannot be removed from the system, due to application dependencies; however, unique administrator accounts have been created, in order to eliminate the need to use all default administrator accounts.		
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**2.1.1** Verify the following regarding vendor default settings for wireless environments:			

	2.1.1.a Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions	Verizon Business reviewed wireless settings within the PCI Reference Architecture Solutions environment and verified the following: Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N		
	2.1.1.b Verify default SNMP community strings on wireless devices were changed.	Verizon Business reviewed wireless settings within the PCI Reference Architecture Solutions environment and verified the following: Default SNMP community strings have been changed and (SNMPv3 is being used).		
	2.1.1.c Verify default passwords/passphrases on access points were changed.	Verizon Business reviewed wireless settings within the PCI Reference Architecture Solutions environment and verified the following: No default passwords exist within the wireless environment. These are entered at initial login. Only unique, non-default accounts exist for interactive administration within the wireless		
	2.1.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.	Verizon Business reviewed wireless settings within the PCI Reference Architecture Solutions environment and verified the following: WPA technology is enabled (WPA/TKIP w/PEAP authentication).		

	2.1.1.e Verify other security-related wireless vendor defaults were changed, if applicable.	Verizon Business reviewed wireless settings within the PCI Reference Architecture Solutions environment and verified the following: No Default SSID exists. This must be entered at initial installation, and is recommended by Cisco to be unique. SSID broadcast was disabled. Wireless management and web mode is disabled.		

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for • Standardization (ISO) • SysAdmin Audit Network Security • (SANS) Institute • National Institute of Standards • Technology (NIST)	**2.2.a** Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.	**N/A** – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the organization / service provider. Verizon Business also observed that network device configurations can be deployed and enforced through Cisco Prime LMS, allowing standardized configurations against secure configuration templates. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N		

		RSA Authentication Manager RSA EnVision Cisco Identity Services Engine Cisco Prime LMS EMC CLARiiON CX-240 Cisco Unified Computing System Cisco UCS Express server on Services Ready Engine Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control **Note:** Verizon Business reviewed configurations across all above mentioned technologies and confirmed they were configured according to best practice standards.		

	2.2.b Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2.	**N/A** – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the organization / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555-x Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R HyTrust Appliance		

		Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N RSA Authentication Manager RSA EnVision Cisco Identity Services Engine Cisco Prime LMS EMC CLARiiON CX-240 Cisco Unified Computing System Cisco UCS Express server on Services Ready Engine Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control **Note:** Verizon Business reviewed configurations across all above mentioned technologies and confirmed they were configured according to best practice standards.		

	2.2.c Verify that system configuration standards are applied when new systems are configured.	**N/A** – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the organization / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R HyTrust Appliance		

		Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N RSA Authentication Manager RSA EnVision Cisco Identity Services Engine Cisco Prime LMS EMC CLARiiON CX-240 Cisco Unified Computing System Cisco UCS Express server on Services Ready Engine Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control **Note:** Verizon Business reviewed configurations across all above mentioned technologies and confirmed they were configured according to best practice standards.		
	2.2.d Verify that system configuration standards include each item below (2.2.1 – 2.2.4).			

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) **Note:** Where virtualization technologies are in use, implement only one primary function per virtual system component.	**2.2.1.a** For a sample of system components, verify that only one primary function is implemented per server.	**N/A** – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the organization / service provider. **Note:** Verizon Business reviewed configurations across all above mentioned technologies and confirmed they were configured according to best practice standards.		
	2.2.1.b If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.	**N/A** – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the organization / service provider.		

2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or ec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	**2.2.2.a** For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that only necessary services or protocols are enabled.	Verizon Business reviewed configuration settings for Cisco's PCI Reference Architecture Solutions and verified that that only necessary services or protocols are enabled. Enforcement of protocol restriction and secure administrative access can be configured through Cisco Prime LMS under Config Transport settings. **Note:** Although Cisco followed a configuration standard to harden the OS for management consoles, Verizon Business did not review those configurations beyond secure administrative access (e.g. https, SSH), audit logging, and password/lockout settings. OS hardening is the responsibility of the organization / service provider, and would vary significantly, depending on OS platform and POS applications deployed. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Integrated Services Routers (ISRs) Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD		

		Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	2.2.2.b Identify any enabled insecure services, daemons, or protocols. Verify they are justified and that security features are documented and implemented.	Verizon Business reviewed configuration settings for PCI Reference Architecture Solutions and verified that insecure services and protocols are not used. **Note:** Although Cisco followed a configuration standard to harden the OS for management consoles, Verizon Business did not review those configurations beyond secure administrative access (e.g. https, SSH), audit logging, and password/lockout settings. OS hardening is the responsibility of the organization / service provider, and would vary significantly, depending on OS platform and POS applications deployed. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Integrated Services Routers (ISRs) Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD		

		Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
2.2.3 Configure system security parameters to prevent misuse.	**2.2.3.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.	Verizon Business interviewed administrators, architects, and SMEs from business units to verify they have knowledge of common security parameters of the system components within the PCI Reference Architecture Solutions environment.		

	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.	**N/A** – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the organization / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		Documentation and implementation of system configuration standards is the responsibility of the organization / service provider.

		Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Video Surveillance Cisco Physical Access Control		

	2.2.3.c For a sample of system components, verify that common security parameters are set appropriately.	Verizon Business reviewed configuration settings across all PCI Reference Architecture Solutions and confirmed they were based on best practice standards, and that common security parameters were set appropriately. Verizon Business also confirmed all management consoles were configured to support secure access (e.g. SSH, https, High-Encryption RDP), and that http, Telnet, and other insecure protocols commonly used for administrative access had been disabled. Additionally, role-based administration was configured for administration of the PCI Reference Architecture Solutions. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch		Server hardening, including appropriate security settings for all system components, is the responsibility of the organization / service provider.

		Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Video Surveillance Cisco Physical Access Control		

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.4.a** For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.	Verizon Business reviewed configurations across all PCI Reference Architecture Solutions and verified that they were based on best practice standards, and that all unnecessary functionality was disabled. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		Server hardening, including appropriate security settings for all system components, is the responsibility of the organization / service provider.

		Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	2.2.4.b. Verify enabled functions are documented and support secure configuration.	Verizon Business reviewed configurations across all PCI Reference Architecture Solutions and confirmed that enabled functions are documented and support secure configuration. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		Server hardening, including appropriate security settings for all system components, is the responsibility of the organization / service provider.

		Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	2.2.4.c. Verify that only documented functionality is present on the sampled system components.	Verizon Business reviewed configurations across all PCI Reference Architecture Solutions and confirmed that only documented functionality is present on the sampled system components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		Server hardening, including appropriate security settings for all system components, is the responsibility of the organization / service provider.

		Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non- console administrative access.	**2.3** For a sample of system components, verify that non-console administrative access is encrypted by performing the following:			

	2.3.a Observe an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested.	Verizon Business reviewed non-console administrative access for all PCI Reference Architecture Solutions and verified that strong encryption methods are invoked before the administrator's password is requested. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD		**Note:** Verification of telnet presence within the management consoles (Windows Server 2003) was not performed. This is the responsibility of the organization / service provider, as part of secure configuration standard processes.

		Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	2.3.b Review services and parameter files on systems to determine that Telnet and other remote login commands are not available for use internally.	Verizon Business reviewed non-console administrative access for all PCI Reference Architecture Solutions and verified that Telnet and other remote login commands are not available for use internally. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		**Note:** Verification of telnet presence within the management consoles (Windows Server 2003) was not performed. This is the responsibility of the organization / service provider, as part of secure configuration standard processes.

		Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	2.3.c Verify that administrator access to the web-based management interfaces is encrypted with strong cryptography.	Verizon Business reviewed non-console administrative access for all PCI Reference Architecture Solutions and verified that administrator access to the web-based management interfaces is encrypted with strong cryptography. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco Video Surveillance Cisco Physical Access Control Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S		**Note:** Verification of telnet presence within the management consoles (Windows Server 2003) was not performed. This is the responsibility of the organization / service provider, as part of secure configuration standard processes.

		Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway SRE – UCS Express server VOIP CUCM Cisco Unified Computing System (UCS) Cisco Secure Access Control Server		
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	**2.4** Perform testing procedures **A.1.1** through **A.1.4** detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (organizations and service providers) hosted environment and data.	**N/A** – For the purpose of this assessment, Cisco is not a hosting provider.		

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows.	**3.1** Obtain and examine the policies, procedures and processes for data retention and disposal, and perform the following:			
3.1.1 Implement a data retention and disposal policy that includes: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements • Processes for secure deletion of data when no longer needed • Specific retention requirements for cardholder data • A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements	**3.1.1.a** Verify that policies and procedures are implemented and include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons).	**N/A** – Data retention / Data disposal policy and procedures is the responsibility of the organization / service provider.		

	3.1.1.b Verify that policies and procedures include provisions for secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data.	**N/A** – Data retention / Data disposal policy and procedures is the responsibility of the organization / service provider.		
	3.1.1.c Verify that policies and procedures include coverage for all storage of cardholder data.	**N/A** – Data retention / Data disposal policy and procedures is the responsibility of the organization / service provider.		
	3.1.1.d Verify that policies and procedures include at least one of the following: A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy. Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy.	**N/A** – Data retention / Data disposal policy and procedures is the responsibility of the organization / service provider.		
	3.1.1.e For a sample of system components that store cardholder data, verify that the data stored does not exceed the requirements defined in the data retention policy.	**N/A** – Data retention / Data disposal policy and procedures is the responsibility of the organization / service provider.		

3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: **Note:** It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.	**3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, verify there is a business justification for the storage of sensitive authentication data, and that the data is secured.	**N/A** – Cisco is not an Issuer and does not support issuing services.		
	3.2.b For all other entities, if sensitive authentication data is received and deleted, obtain and review the processes for securely deleting the data to verify that the data is unrecoverable.	**N/A** – It is the responsibility of the organization to ensure systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted).		
	3.2.c For each item of sensitive authentication data below, perform the following steps:			

3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. **Note:** In the normal course of business, the following data elements from the magnetic stripe may need to be retained: The cardholder's name Primary account number (PAN) Expiration date Service code To minimize risk, store only these data elements as needed for business.	**3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored under any circumstance: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents	**N/A** – It is the responsibility of the organization to ensure systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted).		
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not- present transactions.	**3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three- digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents	**N/A** – It is the responsibility of the organization to ensure systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted).		

3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	**3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents	**N/A** – It is the responsibility of the organization to ensure systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted).		
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). Notes: This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.	**3.3** Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.	**N/A** – Data control and Data classification policies and procedures, including masking PAN data, except for those with a specific need to see full PAN data, is the responsibility of the organization.		

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures **Note:** It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	**3.4.a** Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures	**N/A** – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the organization / service provider. Verizon Business reviewed RSA Data Protection Manager application, related to protecting sensitive data within Cisco's PCI Solution environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable RSA Data Protection Manager – 192-bit 3DES or 256-bit AES encryption. RSA Data Protection Manager – 192-bit 3DES or 128-bit, 192-bit, or 256-bit AES encryption.		
	3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).	**N/A** – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the organization / service provider.		

	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.	**N/A** – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the organization / service provider.			
	3.4.d Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs.	**N/A** – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the organization / service provider.			
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).	Verizon Business reviewed RSA Data Protection Manager, EMC CLARiiON CX-240, Cisco MDS Storage Switches, related to protecting sensitive data within Cisco's PCI Solution environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable. **Note**: Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.			

	3.4.1.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).	Verizon Business reviewed RSA Data Protection Manager, EMC CLARiiON CX-240, Cisco MDS Storage Switches, related to protecting sensitive data within Cisco's PCI Solution environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable. **Note**: Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.		

	3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored. **Note:** If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.	Verizon Business reviewed RSA Data Protection Manager, EMC CLARiiON CX-240, Cisco MDS Storage Switches, related to protecting sensitive data within Cisco's PCI Solution environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable. **Note**: Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.		
3.5 Protect any keys used to secure cardholder data against disclosure and misuse: **Note:** This requirement also applies to key-encrypting keys used to protect data- encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.	**3.5** Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:			

3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**3.5.1** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.	**N/A** – Protection of encryption keys is the responsibility of the organization / service provider. Verizon Business confirmed that restricted access to encryption keys is as follows RSA Data Protection Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported to a key administrator. RSA Data Protection Manager security policies require public key authentication to access key material for encryption/decryption purposes. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	**3.5.2.a** Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.	**N/A** – Protection of encryption keys is the responsibility of the organization / service provider. RSA Data Protection Manager: Key encryption key is stored in memory and data encryption keys are stored in encrypted format within Oracle or MS SQL database. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		
	3.5.2.b Identify key storage locations to verify that keys are stored in the fewest possible locations and forms.	**N/A** – Protection of encryption keys is the responsibility of the organization / service provider. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: **Note:** Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.	**3.6.a** Verify the existence of key-management procedures for keys used for encryption of cardholder data.	**N/A** – Key Management policy and procedures is the responsibility of the organization / service provider.		
	3.6.b For service providers only: If the service provider shares keys with their customers for transmission or storage of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely transmit, store and update customer's keys, in accordance with Requirements 3.6.1 through 3.6.8 below.	**N/A** – Key Management policy and procedures is the responsibility of the organization / service provider.		
	3.6.c Examine the key-management procedures and perform the following:			

3.6.1 Generation of strong cryptographic keys	**3.6.1** Verify that key-management procedures are implemented to require the generation of strong keys.	**N/A** – Key Management policies and procedures is the responsibility of the organization / service provider. Verizon Business confirmed that generation of strong keys is included for the following: RSA Data Protection Manager: 192-bit 3DES or 128-bit/192-bit/256-bit AES keys Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6.2 Secure cryptographic key distribution	**3.6.2** Verify that key-management procedures are implemented to require secure key distribution.	**N/A** – Key Management policies and procedures is the responsibility of the organization / service provider. Verizon Business confirmed that secure distribution of keys is included for the following: RSA Data Protection Manager: All key transfers are done over SSLv3/TLSv1 connections between Key Manager Server and Key Manager Clients. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6.3 Secure cryptographic key storage	**3.6.3** Verify that key-management procedures are implemented to require secure key storage.	**N/A** – Key Management policies and procedures is the responsibility of the organization / service provider. Verizon Business confirmed that secure key storage is included for the following: RSA Data Protection Manager: Key encryption key is stored in memory and data encryption keys are stored in encrypted format within Oracle or MS SQL database. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher- text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	**3.6.4** Verify that key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod.	**N/A** – Key Management policies and procedures is the responsibility of the organization / service provider. Verizon Business confirmed that key rotation capabilities are included for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. **Note:** If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.	**3.6.5.a** Verify that key-management procedures are implemented to require the retirement of keys when the integrity of the key has been weakened.	**N/A** – Key Management policies and procedures is the responsibility of the organization / service provider. Verizon Business confirmed that destruction of keys is included for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined, or delete, when necessary.		
	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.	**N/A** – Key Management policies and procedures is the responsibility of the organization / service provider. Verizon Business confirmed that replacement of known or suspected compromised keys is included for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined necessary.		

	3.6.5.c If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations.	**N/A** – Key Management policies and procedures is the responsibility of the organization / service provider. Verizon Business confirmed that retired or replaced cryptographic keys are retained, and that these keys are not used for encryption operations for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). **Note:** Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	**3.6.6** Verify that manual clear-text key-management procedures require split knowledge and dual control of keys.	**N/A** – Key Management policies and procedures is the responsibility of the organization / service provider. Verizon Business confirmed that split knowledge/dual control of keys is included for the following: RSA Data Protection Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format.		
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	**3.6.7** Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.	**N/A** – Key Management policies and procedures is the responsibility of the organization / service provider. Verizon Business confirmed that prevention of unauthorized substitution of keys is included for the following: RSA Data Protection Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format. Key administration functions can only be access through the Key Manager server, via access controls (authentication) through the RSA Access Manager server.		

3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	**3.6.8** Verify that key-management procedures are implemented to require key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	**N/A** – Key custodian lists are the responsibility of the organization/service provider.		

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, EC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to: • The Internet • Wireless technologies, • Global System for Mobile communications (GSM) • General Packet Radio Service (GPRS)	**4.1** Verify the use of security protocols wherever cardholder data is transmitted or received over open, public networks. Verify that strong cryptography is used during data transmission, as follows:	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions and verified that it uses security protocols wherever cardholder data is transmitted or received over open, public networks. **Note:** Wireless networks have been configured to provide PCI required security necessary to support cardholder traffic. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N		

	4.1.a Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.	**Note:** Verizon Business reviewed wireless settings within the PCI Solution environment to confirm WPA encryption has been implemented for all wireless traffic.		
	4.1.b Verify that only trusted keys and/or certificates are accepted.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions and verified that that only trusted keys and/or certificates are accepted.		
	4.1.c Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions and verified that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.		
	4.1.d Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions and verified that the proper encryption strength is implemented for the encryption methodology in use.		
	4.1.e For SSL/TLS implementations: Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). Verify that no cardholder data is required when HTTPS does not appear in the URL.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions and verified that for SSL/TLS implementations, HTTPS appears as a part of the browser URL		

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. **Note:** The use of WEP as a security control was prohibited as of 30 June 2010.	**4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.	Verizon Business reviewed wireless settings within the PCI Reference Architecture Solutions environment to confirm that WPA encryption has been implemented for all wireless traffic. Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N		
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	**4.2.a** Verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	**N/A** – Data Control / Encryption policy and procedures is the responsibility of the organization / service provider.		
	4.2.b Verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.	**N/A** – Data Control / Encryption policy and procedures is the responsibility of the organization / service provider.		

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business- approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	**N/A** – Deployment of anti-virus software on all servers within the PCI Reference Architecture Solutions environment is the responsibility of the organization / service provider.		
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**5.1.1** For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).	**N/A** – Deployment of anti-virus software on all servers within the PCI Reference Architecture Solutions environment is the responsibility of the organization / service provider.		
5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	**5.2** Verify that all anti-virus software is current, actively running, and generating logs by performing the following:	**N/A** – Deployment of anti-virus software on all servers within the PCI Reference Architecture Solutions environment is the responsibility of the organization / service provider.		
	5.2.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.	**N/A** – Written A/V policy is the responsibility of the organization / service provider.		
	5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.	**N/A** – Deployment of anti-virus software on all servers within the PCI Reference Architecture Solutions environment is the responsibility of the organization / service provider.		

	5.2.c For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.	**N/A** – Deployment of anti-virus software on all servers within the PCI Reference Architecture Solutions environment is the responsibility of the organization / service provider.		
	5.2.d For a sample of system components, verify that antivirus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7	**N/A** – Central storage and retention of A/V logs is the responsibility of the organization / service provider.		

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor- provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI DSS Requirements	Testing Procedures	In Place	Not In Place	Comments

6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. **Note:** An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.	**6.1.a** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.	Verizon Business reviewed configurations for the PCI Reference Architecture Solution components, including management consoles for components within the PCI Solution environment and confirmed they are running current software releases and contain current vendor patches as of the time of this assessment. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X		

		Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.	**N/A** – Patch management policy and procedures is the responsibility of the organization / service provider.		

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Notes: Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component. The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.	**6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities, and that a risk ranking is assigned to such vulnerabilities. (At minimum, the most critical, highest risk vulnerabilities should be ranked as "High."	**N/A** – Patch / Risk management policy and procedures is the responsibility of the organization / service provider.		
	6.2.b Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information.	**N/A** – Patch / Risk management policy and procedures is the responsibility of the organization / service provider. Verizon Business recommends using multiple outside sources (e.g. SANS, CERT, SecurityFocus, vendor websites, etc) to identify new vulnerability issues within the environment.		

6.3 Develop software applications (internal and external, and including web- based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	**6.3.a** Obtain and examine written software development processes to verify that the processes are based on industry standards and/or best practices.	**N/A** – Software Development was not in scope for this assessment.		
	6.3.b Examine written software development processes to verify that information security is included throughout the life cycle.	**N/A** – Software Development was not in scope for this assessment.		
	6.3.c Examine written software development processes to verify that software applications are developed in accordance with PCI DSS.	**N/A** – Software Development was not in scope for this assessment.		
	6.3.d From an examination of written software development processes, and interviews of software developers, verify that:			

6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	**6.3.1** Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers.	**N/A** – Software Development was not in scope for this assessment.		
6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. **Note:** This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	**6.3.2.a** Obtain and review policies to confirm that all custom application code changes must be reviewed (using either manual or automated processes) as follows: Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). Appropriate corrections are implemented prior to release. Code review results are reviewed and approved by management prior to release.	**N/A** – Software Development was not in scope for this assessment.		

	6.3.2.b Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.	**N/A** – Software Development was not in scope for this assessment.		
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	**6.4** From an examination of change control processes, interviews with system and network administrators, and examination of relevant data (network configuration documentation, production and test data, etc.), verify the following:			
6.4.1 Separate development/test and production environments	**6.4.1** The development/test environments are separate from the production environment, with access control in place to enforce the separation.	**N/A** – Software Development was not in scope for this assessment.		
6.4.2 Separation of duties between development/test and production environments	**6.4.2** There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.	**N/A** – Software Development was not in scope for this assessment.		
6.4.3 Production data (live PANs) are not used for testing or development	**6.4.3** Production data (live PANs) are not used for testing or development.	**N/A** – Software Development was not in scope for this assessment.		

6.4.4 Removal of test data and accounts before production systems become active	**6.4.4** Test data and accounts are removed before a production system becomes active.	**N/A** – Software Development was not in scope for this assessment.		
6.4.5 Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	**6.4.5.a** Verify that change-control procedures related to implementing security patches and software modifications are documented and require items 6.4.5.1 – 6.4.5.4 below.	**N/A** – Software Development was not in scope for this assessment.		
	6.4.5.b For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the following:			
6.4.5.1 Documentation of impact.	**6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change.	**N/A** – Security Policy/Procedures (Change Control) is the responsibility of the organization / service provider.		
6.4.5.2 Documented change approval by authorized parties.	**6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change.	**N/A** – Security Policy/Procedures (Change Control) is the responsibility of the organization / service provider.		

6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	**6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.	**N/A** – Security Policy/Procedures (Change Control) is the responsibility of the organization / service provider.		
	6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.	**N/A** – Security Policy/Procedures (Change Control) is the responsibility of the organization / service provider.		
6.4.5.4 Back-out procedures.	**6.4.5.4** Verify that back-out procedures are prepared for each sampled change.	**N/A** – Security Policy/Procedures (Change Control) is the responsibility of the organization / service provider.		

6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: **Note:** The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	**6.5.a** Obtain and review software development processes. Verify that processes require training in secure coding techniques for developers, based on industry best practices and guidance.	**N/A** – Software Development is not in scope for assessment.		
	6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.	**N/A** – Software Development is not in scope for assessment.		
	6.5.c. Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following:			

6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)	**N/A** – Software Development is not in scope for assessment.		
6.5.2 Buffer overflow	**6.5.2** Buffer overflow (Validate buffer boundaries and truncate input strings.)	**N/A** – Software Development is not in scope for assessment.		
6.5.3 Insecure cryptographic storage	**6.5.3** Insecure cryptographic storage (Prevent cryptographic flaws)	**N/A** – Software Development is not in scope for assessment.		
6.5.4 Insecure communications	**6.5.4** Insecure communications (Properly encrypt all authenticated and sensitive communications)	**N/A** – Software Development is not in scope for assessment.		
6.5.5 Improper error handling	**6.5.5** Improper error handling (Do not leak information via error messages)	**N/A** – Software Development is not in scope for assessment.		
6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2). **Note:** This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.	**6.5.6** All "High" vulnerabilities as identified in PCI DSS Requirement 6.2.	**N/A** – Software Development is not in scope for assessment.		

Note: Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):				
6.5.7 Cross-site scripting (XSS)	**6.5.7** Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)	**N/A** – Software Development is not in scope for assessment.		
6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)	**6.5.8** Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object references to users.)	**N/A** – Software Development is not in scope for assessment.		
6.5.9 Cross-site request forgery (CSRF)	**6.5.9** Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.)	**N/A** – Software Development is not in scope for assessment.		

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing a web-application firewall in front of public-facing web applications	**6.6** For public-facing web applications, ensure that either one of the following methods are in place as follows: Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: - At least annually - After any changes - By an organization that specializes in application security - That all vulnerabilities are corrected - That the application is re-evaluated after the corrections Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. **Note:** "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.	**N/A** – Public-facing web applications are not in scope for assessment.		

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	**7.1** Obtain and examine written policy for data control, and verify that the policy incorporates the following:			

7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	**7.1.1** Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.	Verizon Business confirmed privileged user IDs are restricted to the least privileges necessary to perform job functions and exist for the following components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM)		

		HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.1.2 Assignment of privileges is based on individual personnel's job classification and function	**7.1.2** Confirm that privileges are assigned to individuals based on job classification and function (also called "role-based access control" or RBAC).	Verizon Business confirmed privileges are assigned to roles that exist for the following components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance		

		Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.	**7.1.3** Confirm that documented approval by authorized parties is required (in writing or electronically) for all access, and that it must specify required privileges.	Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS		

		Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.1.4 Implementation of an automated access control system	**7.1.4** Confirm that access controls are implemented via an automated access control system.	Verizon Business confirmed automated access controls exist for the following components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM)		

		HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision SSL VPN Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	**7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows:			

7.2.1 Coverage of all system components	**7.2.1** Confirm that access control systems are in place on all system components.	Verizon Business reviewed system components and verified that access control systems are in place on all PCI Reference Architecture Solutions components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM)		

		HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.2.2 Assignment of privileges to individuals based on job classification and function	**7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	Verizon Business reviewed system components and verified that access control systems include role-based privilege assignment for all PCI Reference Architecture Solutions components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E		

		EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.2.3 Default "deny-all" setting **Note:** Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.	**7.2.3** Confirm that the access control systems have a default "deny-all" setting.	Verizon Business reviewed system components and verified that access control systems include default "deny-all" settings on all PCI Reference Architecture Solutions components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 502 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments

8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**8.1** Verify that all users are assigned a unique ID for access to system components or cardholder data.	Verizon Business reviewed access lists on all PCI Reference Architecture Solution components and verified that all users are assigned a unique ID for access to system components or cardholder data. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA EnVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: Something you know, such as a password or passphrase Something you have, such as a token device or smart card Something you are, such as a biometric	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following: Obtain and examine documentation describing the authentication method(s) used. For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).	Verizon Business reviewed authentication methods, including observation of live login attempts and verified that a unique ID and password was required for each authentication attempt to all PCI Reference Architecture Solution components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD		

		Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA EnVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) **Note:** Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.	**8.3** To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that two of the three authentication methods are used.	Verizon Business reviewed these components and verified that two-factor authentication was used for remote access. Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 RSA Authentication Manager with SecurID **Note**: All products that can use RADIUS authentication would be able to use the two-factor authentication capabilities of RSA Authentication Manager with SecurID.		**Note:** Two-factor authentication for all remote access, including for employees, contractors, and third parties, is the responsibility of the organization / service provider.

8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	**8.4.a** For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.	Verizon Business reviewed configuration settings of all PCI Reference Architecture Solution components and verified that passwords are unreadable during transmission and storage. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA EnVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
	8.4.b For service providers only, observe password files to verify that customer passwords are encrypted.	**N/A** – For the purpose of this assessment, Cisco is not a service provider.		

8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:	**8.5** Review procedures and interview personnel to verify that procedures are implemented for user identification and authentication management, by performing the following:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**8.5.1** Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to policy by performing the following: • Obtain and examine an authorization form for each ID. • Verify that the sampled user IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained), by tracing information from the authorization form to the system.	**N/A** – Security policy and procedures (ID / Account Management) is the responsibility of the organization / service provider. Creation of access request (authorization) forms for access to PCI "in scope" systems, including: firewalls, routers, switches, VPNs, AD domain access, servers, databases, and applications, is the responsibility of the organization / service provider.		

8.5.2 Verify user identity before performing password resets.	**8.5.2** Examine password/authentication procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset.	**N/A** – Security policy and procedures (ID / Account Management) is the responsibility of the organization / service provider. Account management / password reset procedures are the responsibility of the organization / service provider.		
8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	**8.5.3** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use.	**N/A** – Security policy and procedures (ID / Account Management) is the responsibility of the organization / service provider. Account management / password reset procedures are the responsibility of the organization / service provider.		
8.5.4 Immediately revoke access for any terminated users.	**8.5.4** Select a sample of users terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.	**N/A** – Processes to ensure prompt revocation of granted access rights and deletion / disabling of user IDs is the responsibility of the organization / service provider.		

8.5.5 Remove/disable inactive user accounts at least every 90 days.	**8.5.5** Verify that inactive accounts over 90 days old are either removed or disabled.	**N/A** – Manual audit procedure or third party ID management tool is the responsibility of the organization / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM)		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

		HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	**8.5.6.a** Verify that any accounts used by vendors to access, support and maintain system components are disabled, and enabled only when needed by the vendor.	**N/A** – No external vendor accounts were identified during the assessment.		
	8.5.6.b Verify that vendor remote access accounts are monitored while being used.	**N/A** – No external vendor accounts were identified during the assessment.		

8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.	**8.5.7** Interview the users from a sample of user IDs, to verify that they are familiar with authentication procedures and policies.	**N/A** – Security Policy (Security Awareness) is the responsibility of the organization / service provider.		

8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	**8.5.8.a** For a sample of system components, examine user ID lists to verify the following: Generic user IDs and accounts are disabled or removed Shared user IDs for system administration activities and other critical functions do not exist Shared and generic user IDs are not used to administer any system components	Verizon Business reviewed user ID lists for all PCI Reference Architecture Solution components and verified that generic or shared user IDs and accounts are not used. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

		Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
	8.5.8.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.	**N/A** – Security Policy (Password policy/procedures) is the responsibility of the organization / service provider.		.

	8.5.8.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.	**N/A** – Security Policy (Password policy/procedures) is the responsibility of the organization / service provider.		

8.5.9 Change user passwords at least every 90 days.	**8.5.9.a** For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture Solutions are configured to change user passwords at least every 90 days. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

		Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Cisco Prime LMS Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	8.5.9.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to change periodically and that non- consumer users are given guidance as to when, and under what circumstances, passwords must change.	**N/A** – For the purpose of this assessment, Cisco is not a service provider.		

8.5.10 Require a minimum password length of at least seven characters.	**8.5.10.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture Solutions are configured to require a minimum password length of at least seven characters. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		UCS-SRE may require compensating controls

		Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
	8.5.10.b For service providers only, review internal processes and customer/user documentation to verify that that non-consumer user passwords are required to meet minimum length requirements.	**N/A** – For the purpose of this assessment, Cisco is not a service provider.		

8.5.11 Use passwords containing both numeric and alphabetic characters.	**8.5.11.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture Solutions are configured to use passwords containing both numeric and alphabetic characters. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

		Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
	8.5.11.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to contain both numeric and alphabetic characters.	**N/A** – For the purpose of this assessment, Cisco is not a service provider.		

8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	**8.5.12.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture Solutions are configured to not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

		Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
	8.5.12.b For service providers only, review internal processes and customer/user documentation to verify that new non-consumer user passwords cannot be the same as the previous four passwords.	**N/A** – For the purpose of this assessment, Cisco is not a service provider.		

8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.5.13.a** For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than six invalid logon attempts.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture Solutions are configured to limit repeated access attempts by locking out the user ID after not more than six attempts. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

		Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
	8.5.13.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user accounts are temporarily locked-out after not more than six invalid access attempts.	**N/A** – For the purpose of this assessment, Cisco is not a service provider.		

8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	**8.5.14** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture Solutions are configured to set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

		Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**8.5.15** For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture Solutions are configured in such a way that If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X		

		Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.	**8.5.16.a** Review database and application configuration settings and verify that all users are authenticated prior to access.	**N/A** – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the organization / service provider.		

	8.5.16.b Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).	**N/A** – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the organization / service provider.		
	8.5.16.c Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators.	**N/A** – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the organization / service provider.		
	8.5.16.d Review database applications and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).	**N/A** – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the organization / service provider.		

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco Video Surveillance Cisco Physical Access Control		
9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. **Note:** "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.	**9.1.1.a** Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco Video Surveillance Cisco Physical Access Control		

	9.1.1.b Verify that video cameras and/or access control mechanisms are protected from tampering or disabling.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
	9.1.1.c Verify that video cameras and/or access control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.1.2 Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.	**9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized onsite personnel. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco Identity Services Engine Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Unified Communications Manager and IP Phones		

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	**9.2.a** Review processes and procedures for assigning badges to onsite personnel and visitors, and verify these processes include the following: requirements, and Revoking terminated onsite personnel and expired visitor badges	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
	9.2.b Verify that access to the badge system is limited to authorized personnel.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
	9.2.c Examine badges in use to verify that they clearly identify visitors and it is easy to distinguish between onsite personnel and visitors.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.3 Make sure all visitors are handled as follows:	**9.3** Verify that visitor controls are in place as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained.	**9.3.1** Observe the use of visitor ID badges to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		

9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.	**9.3.2.a** Observe people within the facility to verify the use of visitor ID badges, and that visitors are easily distinguishable from onsite personnel.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
	9.3.2.b Verify that visitor badges expire.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.	**9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	**9.4.a** Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and is retained for at least three months.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		

9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.	**9.5.a** Observe the storage location's physical security to confirm that backup media storage is secure.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
	9.5.b Verify that the storage location security is reviewed at least annually.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.6 Physically secure all media.	**9.6** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	**9.7** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.7.1 Classify media so the sensitivity of the data can be determined.	**9.7.1** Verify that all media is classified so the sensitivity of the data can be determined.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.	**9.7.2** Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		

9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	**9.8** Select a recent sample of several days of offsite tracking logs for all media, and verify the presence in the logs of tracking details and proper management authorization.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.9 Maintain strict control over the storage and accessibility of media.	**9.9** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	**9.9.1** Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.10 Destroy media when it is no longer needed for business or legal reasons as follows:	**9.10** Obtain and examine the periodic media destruction policy and verify that it covers all media, and confirm the following:	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	**9.10.1.a** Verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		

	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a "to-be-shredded" container has a lock preventing access to its contents.	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	**9.10.2** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).	**N/A** – Security Policy/Procedures (Physical Security) is the responsibility of the organization / service provider.		

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that audit trails are enabled and active on all PCI Reference Architecture Solutions. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD		

		Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews, examination of audit logs, and examination of audit log settings, perform the following:			

10.2.1 All individual accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that all individual access to cardholder data and/or access to the cardholder data environment is logged. As cardholder data applications are outside of the scope of this assessment, validated system components were assessed to determine the ability to capture access to the cardholder data environment, which complements the overall cardholder data environment audit trail. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD		

		Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Verify actions taken by any individual with root or administrative privileges are logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that actions taken by any individual with root or administrative privileges are logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD		

		Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2.3 Access to all audit trails	**10.2.3** Verify access to all audit trails is logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that access to all audit trails is logged. Verizon Business observed system-generated configuration output for the following system components: Cisco Security Manager HyTrust Appliance Cisco WCS Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Unified Communications Manager Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2.4 Invalid logical access attempts	**10.2.4** Verify invalid logical access attempts are logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that invalid logical access attempts are logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2 5 Use of identification and authentication mechanisms	**10.2.5** Verify use of identification and authentication mechanisms is logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that use of identification and authentication mechanisms is logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on ServicesReady Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2.6 Initialization of the audit logs	**10.2.6** Verify initialization of audit logs is logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that initialization of audit logs is logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

		Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2.7 Creation and deletion of system-level objects	**10.2.7** Verify creation and deletion of system level objects are logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that creation and deletion of system level objects are logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

		Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Through interviews and observation, for each auditable event (from 10.2), perform the following:			

10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that user identification is included in log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that type of event is included in log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3.3 Date and time	**10.3.3** Verify date and time stamp is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that date and time stamp is included in log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that success or failure indication is included in log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that origination of event is included in log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

		Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3.6 Identity or name of affected data, system component, or resource.	**10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture Solutions to verify that identity or name of affected data, system component, or resources is included in the log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. **Note:** One example of time synchronization technology is Network Time Protocol (NTP).	**10.4.a** Verify that time-synchronizatio n technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that NTP is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.		

	10.4.b Obtain and review the process for acquiring, distributing and storing the correct time within the organization, and review the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:			

10.4.1 Critical systems have the correct and consistent time.	**10.4.1.a** Verify that only designated central time servers receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that only designated central time servers receive time signals from external sources, and time signals from external sources are based on universally accepted time. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	10.4.1.b Verify that the designated central time servers peer with each other to keep accurate time, and other internal servers receive time only from the central time servers.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that the designated central time servers peer with each other to keep accurate time, and other internal servers receive time only from the central time servers. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X		

		Cisco Catalyst 4507+R Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.4.2 Time data is protected.	**10.4.2.a** Review system configurations and time-synchronizatio n settings to verify that access to time data is restricted to only personnel with a business need to access time data.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that access to time data is restricted to only personnel with a business need to access time data Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

		Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	10.4.2.b Review system configurations and time synchronization settings and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that any changes to time settings on critical systems are logged, monitored, and reviewed. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

		Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.4.3 Time settings are received from industry-accepted time sources.	**10.4.3** Verify that the time servers accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that the time servers accept time updates from specific, industry-accepted external sources. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

		Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
10.5 Secure audit trails so they cannot be altered.	**10.5** Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that audit trails are secured so that they cannot be altered as follows:		

10.5.1 Limit viewing of audit trails to those with a job-related need.	**10.5.1** Verify that only individuals who have a job-related need can view audit trail files.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that only individuals who have a job-related need can view audit trail files. Verizon Business observed system-generated configuration output for the following system components: Cisco Security Manager HyTrust Appliance Cisco WCS Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Unified Communications Manager Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		
10.5.2 Protect audit trail files from unauthorized modifications.	**10.5.2** Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. Verizon Business observed system-generated configuration output for the following system components: RSA enVision		

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that current audit trail files are promptly backed up to a centralized log server that is difficult to alter. Verizon Business observed system-generated configuration output for the following system components: Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express server on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	**10.5.4** Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that logs for external-facing technologies are sent to a secure centralized internal log server. Verizon Business observed system-generated configuration output for the following external-facing system and central audit trail components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Virtual Service Gateway Cisco ASA Services Module Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E RSA Authentication Manager RSA enVision Cisco Identity Services Engine Cisco Prime LMS		

10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	**10.5.5** Verify the use of file-integrity monitoring or change- detection software for logs by examining system settings and monitored files and results from monitoring activities.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that use of file-integrity monitoring software for logs by examining system settings and monitored files and results from monitoring activities. Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Communications Manager and IP Phones Cisco Video Surveillance Cisco Physical Access Control Cisco Unified Computing System (UCS) RSA Authentication Manager Cisco Security Manager RSA Data Protection Manager Cisco MDS Storage Switches EMC CLARiiON CX-240 Cisco Secure Access Control Server Cisco Prime LMS		Note: This requirement is met by the use of the RSA enVision server aggregating each of the device logs and file integrity monitoring being provided by the RSA enVision software.
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). **Note:** Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.	**10.6.a** Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.	**N/A** – Policies and Procedures is the responsibility of the organization / service provider.		

	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components.	Verizon Business reviewed configuration settings of PCI Reference Architecture Solutions to verify that log aggregation solutions generate events and alerts which are reviewed daily.		
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	**10.7.a** Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.	**N/A** – Security Policy (Data Retention) is the responsibility of the organization / service provider.		
	10.7.b Verify that audit logs are available for at least one year and processes are in place to immediately restore at least the last three months' logs for analysis.	Verizon Business reviewed online logs and audit trail archive methods within the PCI Reference Architecture Solutions environment to confirm that audit trails can be retained for at least one year, with at least three months available online.		

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. **Note:** Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.	**11.1.a** Verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis.	Verizon Business confirmed that wireless controllers are configured to continually scan and detect rogue APs and wireless devices.		

	11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: WLAN cards inserted into system components Portable wireless devices connected to system components (for example, by USB, etc.) Wireless devices attached to a network port or network device	Verizon Business verified that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: WLAN cards inserted into system components Portable wireless devices connected to system components (for example, by USB, etc.) Wireless devices attached to a network port or network device Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E Cisco Identity Services Engine Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

	11.1.c Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities.	**N/A** – Policy and procedures is the responsibility of the organization / service provider.		
	11.1.d If automated monitoring is utilized (for example, wireless IDS/, NAC, etc.), verify the configuration will generate alerts to personnel.	Verizon Business verified If automated monitoring is utilized, the configuration will generate alerts to personnel. Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N Cisco Identity Services Engine Cisco switches-branch Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

	11.1.e Verify the organization's incident response plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.	**N/A** – Incident Response policy and procedures is the responsibility of the organization / service provider.		
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component Installations, changes in network topology, firewall rule modifications, product upgrades). **Note:** It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re- scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.	**11.2** Verify that internal and external vulnerability scans are performed as follows:			

11.2.1 Perform quarterly internal vulnerability scans.	**11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.	**N/A** – Internal quarterly scanning is the responsibility of the organization / service provider.		
	11.2.1.b Review the scan reports and verify that the scan process includes rescans until passing results are obtained, or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.	**N/A** – Internal quarterly scanning is the responsibility of the organization / service provider.		
	11.2.1.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**N/A** – Internal quarterly scanning is the responsibility of the organization / service provider.		

11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). **Note:** Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.	**11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period.	**N/A** – Third party external, quarterly scanning is the responsibility of the organization / service provider.		
	11.2.2.b Review the results of each quarterly scan to ensure that they satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures).	**N/A** – Third party external, quarterly scanning is the responsibility of the organization / service provider.		
	11.2.2.c Review the scan reports to verify that the scans were completed by an Approved Scanning Vendor (ASV), approved by the PCI SSC.	**N/A** – Third party external, quarterly scanning is the responsibility of the organization / service provider.		

11.2.3 Perform internal and external scans after any significant change. **Note:** Scans conducted after changes may be performed by internal staff.	**11.2.3.a** Inspect change control documentation and scan reports to verify that system components subject to any significant change were scanned.	**N/A** – Third party external scanning / Internal scanning is the responsibility of the organization / service provider.		
	11.2.3.b Review scan reports and verify that the scan process includes rescans until: For external scans, no vulnerabilities exist that are scored greater than a 4.0 by the CVSS, For internal scans, a passing result is obtained or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.	**N/A** – Third party external scanning / Internal scanning is the responsibility of the organization / service provider.		
	11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**N/A** – Third party external scanning / Internal scanning is the responsibility of the organization / service provider.		

11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub- network added to the environment, or a web server added to the environment). These penetration tests must include the following:	**11.3.a** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.	**N/A** – Penetration Testing is the responsibility of the organization / service provider.		
	11.3.b Verify that noted exploitable vulnerabilities were corrected and testing repeated.	**N/A** – Penetration Testing is the responsibility of the organization / service provider.		
	11.3.c Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**N/A** – Penetration Testing is the responsibility of the organization / service provider.		
11.3.1 Network-layer penetration tests	**11.3.1** Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems.	**N/A** – Penetration Testing is the responsibility of the organization / service provider.		

11.3.2 Application-layer penetration tests	**11.3.2** Verify that the penetration test includes application-layer penetration tests. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.	**N/A** – Penetration Testing is the responsibility of the organization / service provider.		
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	**11.4.a** Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored.	Verizon Business reviewed all IDS/ within the PCI Reference Architecture Solutions environment and confirmed that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5555 Cisco ASA 5500 Series-branch Cisco ASA 5515-x Cisco Intrusion Detection Services Module Cisco routers-branch Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945		
	11.4.b Confirm IDS and/or are configured to alert personnel of suspected compromises.	Verizon Business reviewed all IDS/ within the PCI Reference Architecture Solutions environment and confirmed that they are configured to alert personnel of suspected compromises.		

	11.4.c Examine IDS/ configurations and confirm IDS/ devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.	Verizon Business reviewed all IDS/ within the PCI Reference Architecture Solutions environment and confirmed that they are configured, maintained, and updated per vendor instructions to ensure optimal protection.		
11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. **Note:** For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the organization or service provider).	**11.5.a** Verify the use of file-integrity monitoring tools within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files	Verizon Business reviewed FIM settings, monitored files, and results from monitoring activities within the PCI Reference Architecture Solutions environment and verified that file-integrity monitoring tools are used.		

	11.5.b Verify the tools are configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.	Verizon Business reviewed FIM settings, monitored files, and results from monitoring activities within the PCI Reference Architecture Solutions environment and verified that FIM is to be configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly by the organization or service provider.		

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).	**N/A** – Security Policy is the responsibility of the organization / service provider.		
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.	**N/A** – Security Policy is the responsibility of the organization / service provider.		

12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)	**12.1.2.a** Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.	**N/A** – Security Policy is the responsibility of the organization / service provider.		
	12.1.2.b Review risk assessment documentation to verify that the risk assessment process is performed at least annually.	**N/A** – Security Policy is the responsibility of the organization / service provider.		
12.1.3 Includes a review at least annually and updates when the environment changes.	**12.1.3** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.	**N/A** – Security Policy is the responsibility of the organization / service provider.		
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	**12.2** Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.	**N/A** – Security Policy and Procedures is the responsibility of the organization / service provider.		

12.3 Develop usage policies for critical technologies (for example, remote- access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following:	**12.3** Obtain and examine the usage policies for critical technologies and perform the following:			
12.3.1 Explicit approval by authorized parties	**12.3.1** Verify that the usage policies require explicit approval from authorized parties to use the technologies.	**N/A** – Acceptable Use Policy is the responsibility of the organization / service provider.		
12.3.2 Authentication for use of the technology	**12.3.2** Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token).	**N/A** – Acceptable Use Policy is the responsibility of the organization / service provider.		
12.3.3 A list of all such devices and personnel with access	**12.3.3** Verify that the usage policies require a list of all devices and personnel authorized to use the devices.	**N/A** – Acceptable Use Policy is the responsibility of the organization / service provider.		
12.3.4 Labeling of devices to determine owner, contact information and purpose	**12.3.4** Verify that the usage policies require labeling of devices with information that can be correlated to owner, contact information and purpose.	**N/A** – Acceptable Use Policy / Asset List is the responsibility of the organization / service provider.		
12.3.5 Acceptable uses of the technology	**12.3.5** Verify that the usage policies require acceptable uses for the technology.	**N/A** – Acceptable Use Policy is the responsibility of the organization / service provider.		

12.3.6 Acceptable network locations for the technologies	**12.3.6** Verify that the usage policies require acceptable network locations for the technology.	**N/A** – Acceptable Use Policy is the responsibility of the organization / service provider.		
12.3.7 List of company-approved products	**12.3.7** Verify that the usage policies require a list of company-approved products.	**N/A** – Acceptable Use Policy is the responsibility of the organization / service provider.		
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**12.3.8** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	**N/A** – Acceptable Use / Remote Access Policy is the responsibility of the organization / service provider.		
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	**12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	**N/A** – Acceptable Use / Remote Access Policy is the responsibility of the organization / service provider.		
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	**12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	**N/A** – Acceptable Use / Remote Access Policy is the responsibility of the organization / service provider.		
	12.3.10.b For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.	**N/A** – Acceptable Use / Remote Access Policy is the responsibility of the organization / service provider.		

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**12.4** Verify that information security policies clearly define information security responsibilities for all personnel.	**N/A** – Security Policy is the responsibility of the organization / service provider.		
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:	**N/A** – Security Policy is the responsibility of the organization / service provider.		
12.5.1 Establish, document, and distribute security policies and procedures.	**12.5.1** Verify that responsibility for creating and distributing security policies and procedures is formally assigned.	**N/A** – Security Policy is the responsibility of the organization / service provider.		
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.	**N/A** – Security Policy (Risk / Vulnerability management) is the responsibility of the organization / service provider.		

12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**12.5.3** Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.	**N/A** – Security Policy (Risk / Vulnerability management) is the responsibility of the organization / service provider.		
12.5.4 Administer user accounts, including additions, deletions, and modifications	**12.5.4** Verify that responsibility for administering user account and authentication management is formally assigned.	**N/A** – Security Policy (ID / Account management) is the responsibility of the organization / service provider.		
12.5.5 Monitor and control all access to data.	**12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned.	**N/A** – Security Policy (Data Control / Monitoring) is the responsibility of the organization / service provider.		
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	**12.6.a** Verify the existence of a formal security awareness program for all personnel.	**N/A** – Security Policy (Security Awareness) is the responsibility of the organization / service provider.		
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:			
12.6.1 Educate personnel upon hire and at least annually. **Note:** Methods can vary depending on the role of the personnel and their level of access to the cardholder data.	**12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions).	**N/A** – Security Policy (Security Awareness) is the responsibility of the organization / service provider.		

	12.6.1.b Verify that personnel attend awareness training upon hire and at least annually.	**N/A** – Security Policy (Security Awareness) is the responsibility of the organization / service provider.		
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	**12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.	**N/A** – Security Policy (Security Awareness) is the responsibility of the organization / service provider.		
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) **Note:** For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	**12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential personnel prior to hire who will have access to cardholder data or the cardholder data environment.	**N/A** – Security Policy (Background Checks) is the responsibility of the organization / service provider.		

12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	**12.8** If the entity shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following:			
12.8.1 Maintain a list of service providers.	**12.8.1** Verify that a list of service providers is maintained.	**N/A** – Connected Entity List (List of Service Providers with whom cardholder data is shared) is the responsibility of the organization / service provider.		
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	**12.8.2** Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.	**N/A** – Third party contracts is the responsibility of the organization / service provider.		
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**12.8.3** Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider.	**N/A** – Policies and Procedures for sharing cardholder data with third parties / Service Providers is the responsibility of the organization / service provider.		
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**12.8.4** Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.	**N/A** – Policies and Procedures for sharing cardholder data with third parties / Service Providers is the responsibility of the organization / service provider.		

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.9** Obtain and examine the Incident Response Plan and related procedures and perform the following:			
12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data back-up processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands	**12.9.1.a** Verify that the incident response plan includes: -Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum: • Specific incident response procedures • Business recovery and continuity procedures • Data back-up processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands	**N/A** – Incident Response policy and procedures is the responsibility of the organization / service provider.		
	12.9.1.b Review documentation from a previously reported incident or alert to verify that the documented incident response plan and procedures were followed.	**N/A** – Incident Response policy and procedures is the responsibility of the organization / service provider.		
12.9.2 Test the plan at least annually.	**12.9.2** Verify that the plan is tested at least annually.	**N/A** – Incident Response policy and procedures is the responsibility of the organization / service provider.		

12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**12.9.3** Verify through observation and review of policies, that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.	**N/A** – Incident Response policy and procedures is the responsibility of the organization / service provider.		
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	**12.9.4** Verify through observation and review of policies that staff with responsibilities for security breach response is periodically trained.	**N/A** – Incident Response policy and procedures is the responsibility of the organization / service provider.		
12.9.5 Include alerts from intrusion-detection, intrusion-prevention, and file- integrity monitoring systems.	**12.9.5** Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.	**N/A** – Incident Response policy and procedures is the responsibility of the organization / service provider.		
12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**12.9.6** Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**N/A** – Incident Response policy and procedures is the responsibility of the organization / service provider.		

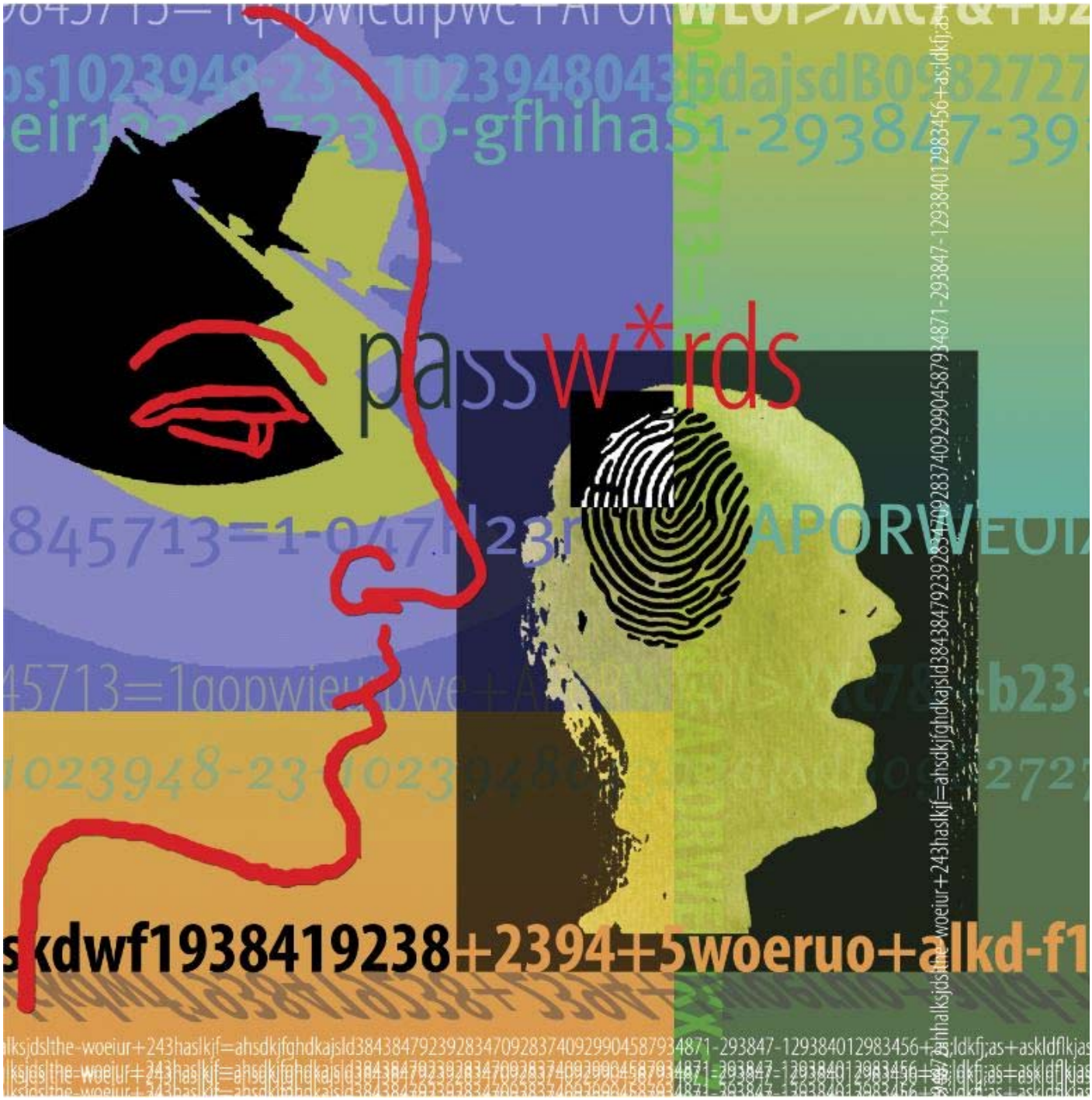


APPENDIX D

The Art of Compliance

Cisco's Global Retail Marketing team commissioned professional artists to create works of art inspired by PCI as a creative way to support Cisco's global launch of the Cisco PCI solution. Each artist was given a description of the 12 requirements of PCI, general networking information, an overview of data security, and a description of Cisco's PCI solution. The following pages contain the artists' interpretations of the solution, networking, and data security.

To learn more, visit: www.cisco.com/go/pci2.


passw*rds
skdwf1938419238+2394=5woeruo+alkd-f1

Artist: Nancy Nimoy

Title: "Encrypted Data Crooks"

This piece is about encrypted data and the bad guys who steal it. When I thought of encrypted data, I thought of a human fingerprint and how it is literally a manifestation of what is inviolably unique about us. I thought to depict one's interior and deeply personal DNA. To communicate how our uniqueness is so often diminished and violated and "stolen" these days.

I used the universal symbol of theft, the generic black-cloaked burglar. He lurks behind the scrim of a loosely drawn human profile, encroaching upon the imperfect water color of a human head with its fingerprint brain. Layers of my piece are deliberately transparent and overlapping to convey "intrusion."

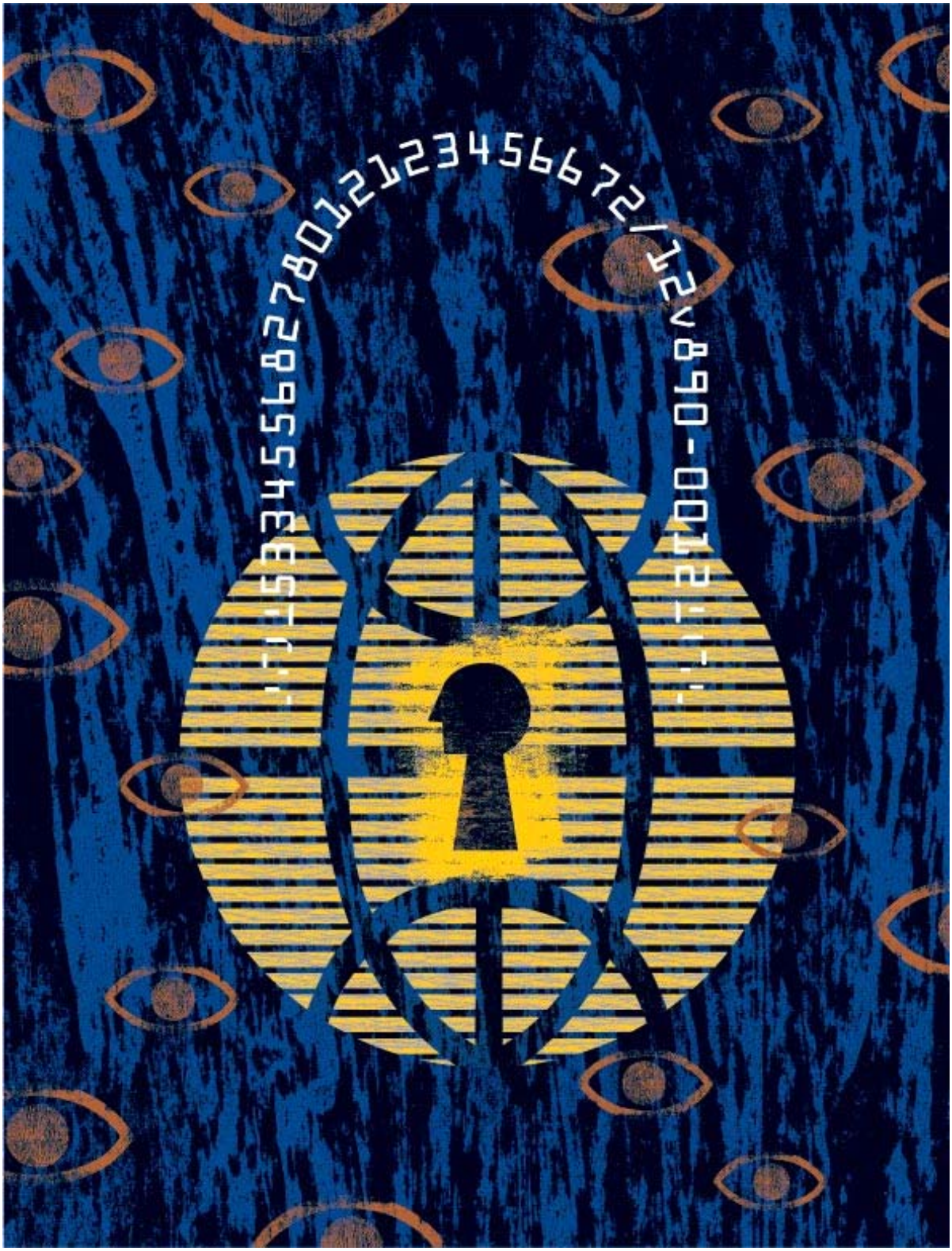
A cacophony of numbers, letters, codes, and secret passwords represent our pathetic defense against the onslaught of HTML bad guys trying to steal our encrypted data.


PCI
"INFORMATION LOCK DOWN"

Artist: Eric Thorsen

Title: "Information Lock Down"

The credit card contained inside the lock illustrates how personal data can be withheld and protected from anyone not having the correct "key" or password. Restricting access to data with user IDs and passwords secures lock doors where sensitive data is stored.



Artist: Matt Foster

Title: "Worldwide Data Safety"

Since the subject is technical in nature, this project needed subtlety and a connection to human elements. Since the image was planned for a myriad of viewing possibilities and would also be viewed worldwide, it needed to illustrate the complex, layered concept of the product yet be simple.

I started with a dark background, adding a layer of semi-transparent red eyes representing the checks and balances of the program, and also doubling as a "who else is looking" aspect. The lock is in the shape of the globe with the numbers being the security element. The keyhole is YOU- the user. The circle completes the world of secure data.


HELBANC
0360 8020 5609 4035

Artist: Lance Jackson

Title: "Stack"

A stack of credit cards is completely tantalizing eye candy. Credit cards are as American as apple pie and baseball. The bright pop-art colors are appropriately American. Knowing that the cards are secured wherever they are used is even more empowering.


LARRY JANOFF ©

Artist: Larry Janoff

Title: "Failed Breach"

I was raised before the computer era, so conceptualizing a breach in security brings to my mind the "olden tools" used by a thief in the "olden days." PCI is a difficult concept for people like me to comprehend, but the theme is SECURITY!



Artist: Sue Averell

Title: "Network Neighborhood"

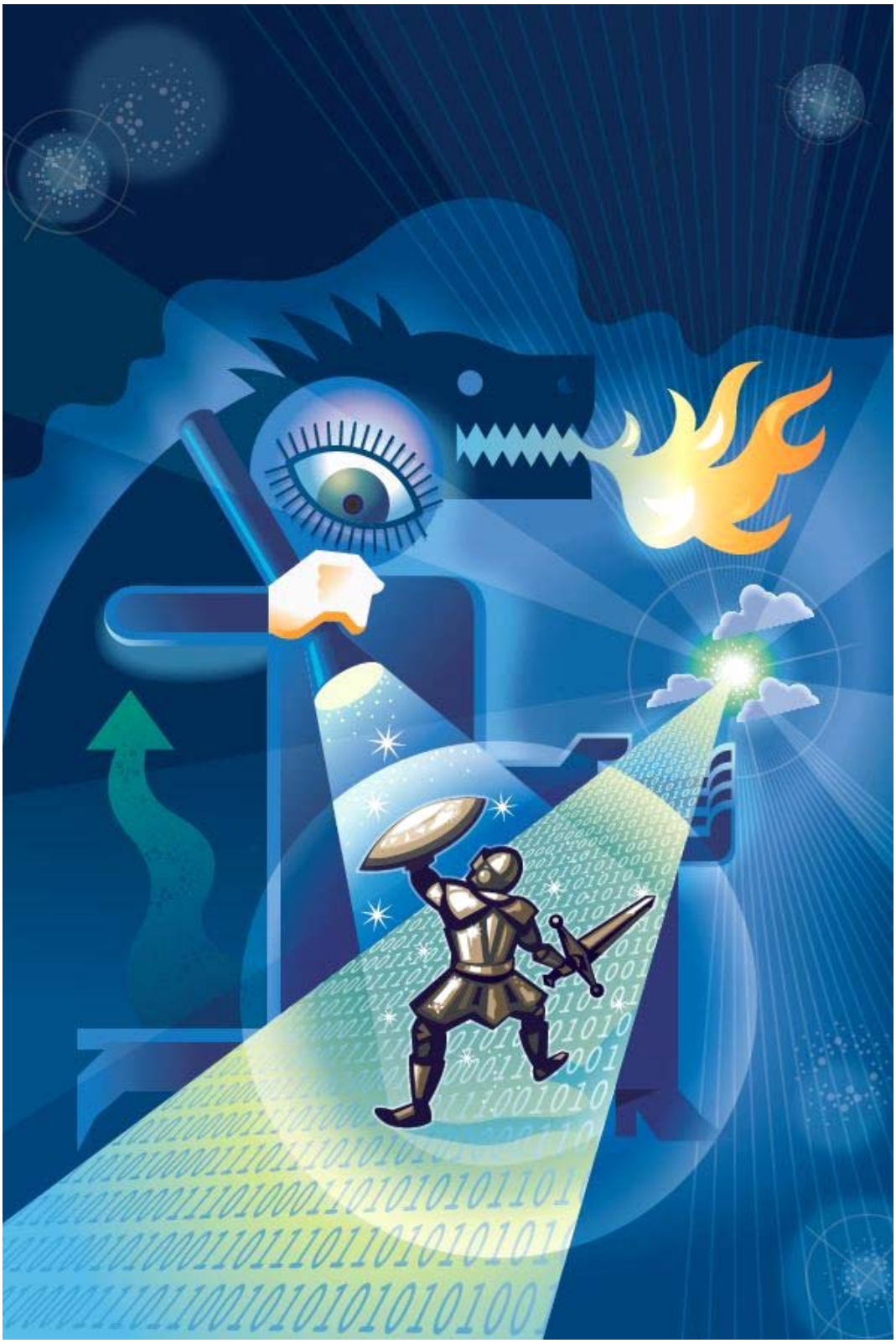
While creating this painting, I strove to combine my current theme of neighborhoods with that of data networks. It was important to me to be true to my style. Color and texture and an elevated view of the subject are some of the identifying characteristics of all my work.


PCI

Artist: Eric Thorsen

Title: "Impenetrable Firewall"

The sculpture of the fist attempting to break through the firewall, but being prevented from doing so, illustrates the basic strength of the essential software called a firewall. Personal computers and corporate computers alike require protection from predators, viruses, and software created to gather such data for ill purposes, including stealing money, data, or personal identities.



Artist: Filip Yip

Title: "Hacker"

Transferring private and important data over the Internet can expose users to the prying and hacking of ruthless cyber-criminals. There is an urgent need for a comprehensive solution to secure the safe transmission of information from point A to B. This godsend will be the cavalier who fights hackers incessantly, and strives to slay the dragon who has been devouring the most valuable and vulnerable asset of all netizens.


PCI
PCI
ADVANCED HACKING
LARRY JANOFF ©
"THEY don't sleep at night"
Larry Janoff

Artist: Larry Janoff

Title: "THEY don't sleep at night"

I visualize a hacker as a vicious creature. I thought it humorous to represent him as a weird, evil monster that is trying very hard to breach PCI Security, someone who never sleeps, day or night.


Carte

Artist: Randy South

Title: "Secure Flight"

The objective of the work is to show that despite the dangers of maintaining financial security, freedom of commerce is still possible.


06/13

Artist: Lance Jackson

Title: "Secure Card"

Having your colorful, expressionistic, inner shopping self literally secured with chains and a lock says it all. You have the power to unlock it. No one else has that key.


PCI
PCI

Artist: Lance Jackson

Title: "Happy Network"

Shopping without information or a connection can be a dizzying, spinning experience. Why be sad or mad when you can be glad? By shopping on a secure networking you become a happy, smiling shopper. Being connected is the new shopping mantra.


PCI

Artist: Jerry Sprunger

Title: "Sanctuary"

The various components in this airbrushed painting serve to exhibit the security, service and reliability of Cisco's PCI solution.

The credit cards and sensitive data behind the firewall on top of the rock pillar are secure due to the inaccessibility provided by two firewalls and secure pathways.The other globe-topped pillars in the background indicate the global coverage the systems offers. The bright light on the horizon is indicative of a bright, secure and strong future.